Qualys. Enterprise

# SAMPLE Spectre/Meltdown Tracking Report

January 17, 2018

This report was generated with an evaluation version of Qualys

| Report Summary | |
|---|---|
| User Name: | Debra Fezza Reed |
| Company: | TAM Demo Account |
| User Role: | Manager |
| Address: | 1600 Bridge Parkway |
| City: | Redwood Shores |
| State: | California |
| Zip: | 94065 |
| Country: | United States of America |
| Created: | 01/17/2018 at 02:45:17 PM (GMT-0800) |
| Template Title: | Spectre/Meltdown Tracking Report |
| Asset Groups: | All |
| IPs: | - |
| Sort by: | Host |
| Trend Analysis: | Custom Date (12/31/2017) |
| Date Range: | 12/31/2017 - 01/17/2018 |
| Active Hosts: | 27 |
| Hosts Matching Filters: | 20 |

## Summary of Vulnerabilities

| Vulnerabilities Total | Security Risk (Avg) | Business Risk |
|---|---|---|
| 30 (+6) | 3.8 | 32/100 |

**by Status**

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 2 | - | 2 |
| Active | 4 | - | 4 |
| Re-Opened | 0 | - | 0 |
| Total | 6 | - | 6 |
| Fixed | 10 | - | 10 |
| Changed | 12 | - | 12 |

**by Severity**

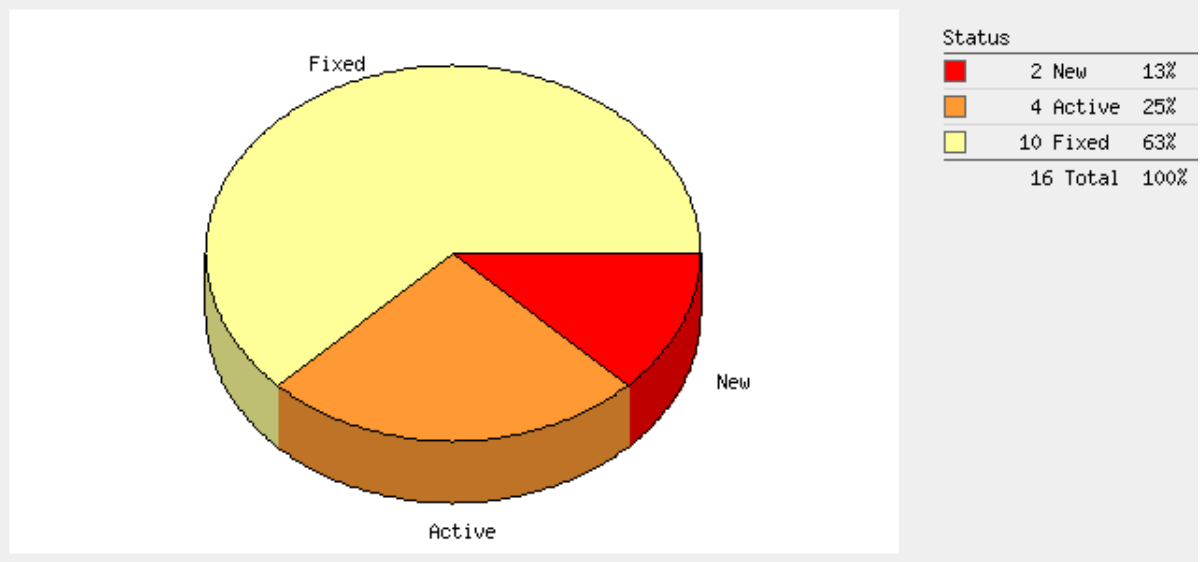
| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 5 | (+5) | - | | 0 | 5 | (+5) |
| 3 | 1 | (+1) | - | | 0 | 1 | (+1) |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 24 | 24 | (0) - |
| Total | 6 | (+6) | - | | 24 | 30 | (+6) |

**5 Biggest Categories**

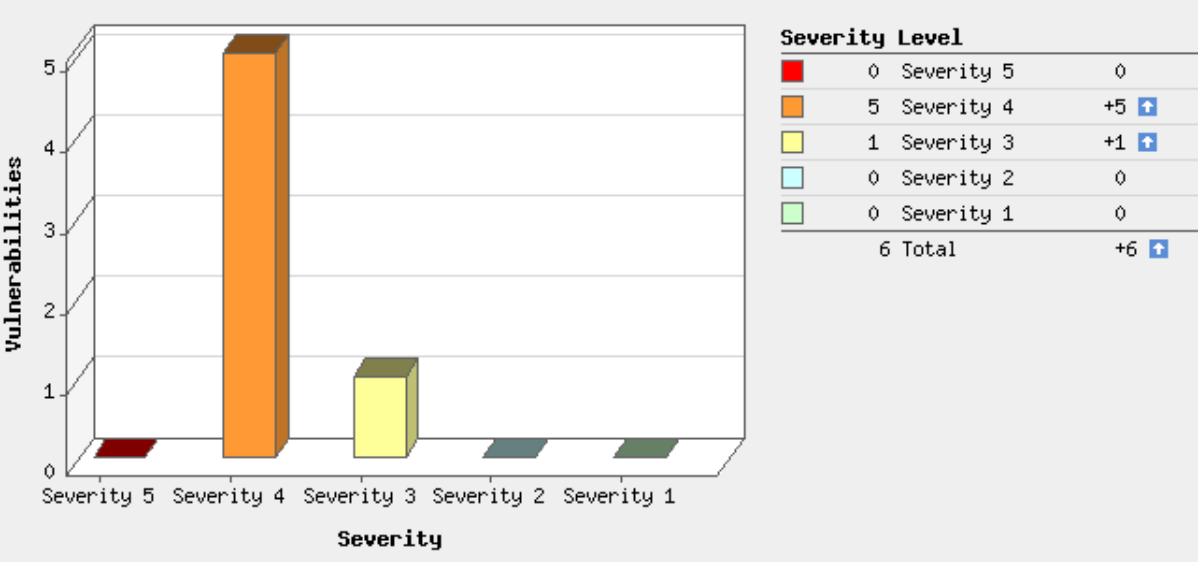
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| Hardware | 0 | (0) - | - | | 13 | 13 | (0) - |
| SMB / NETBIOS | 0 | (0) - | - | | 7 | 7 | (0) - |

| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| Windows | 1 | (+1) | - | | 2 | 3 | (+1) |
| Local | 3 | (+3) | - | | 0 | 3 | (+3) |
| Security Policy | 0 | (0) - | - | | 2 | 2 | (0) - |
| Total | 4 | (+4) | - | | 24 | 28 | (+4) |

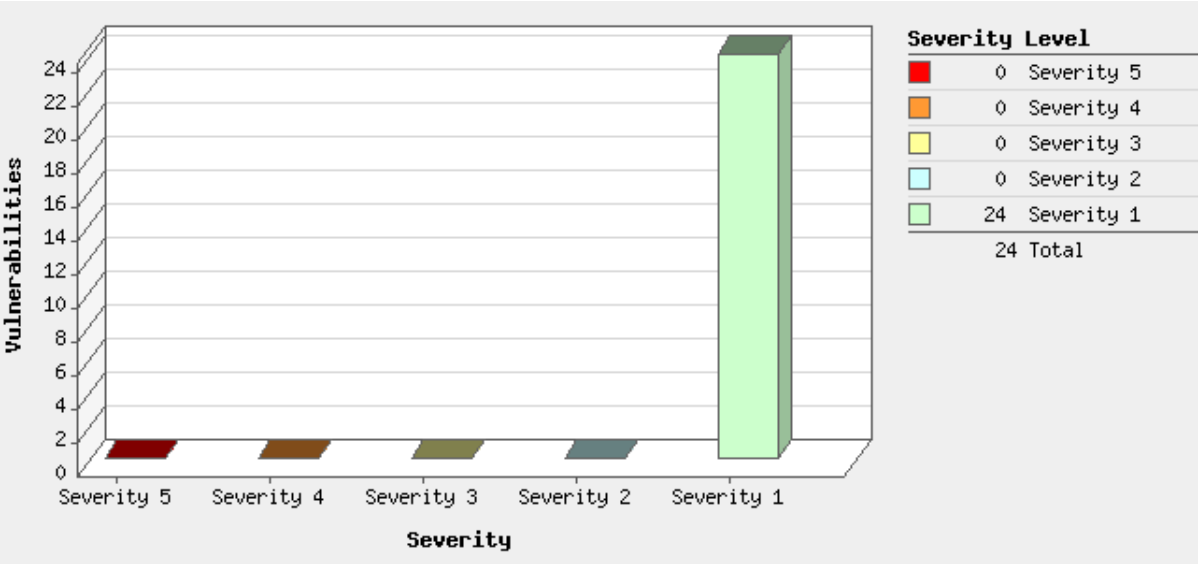
## Vulnerabilities by Status



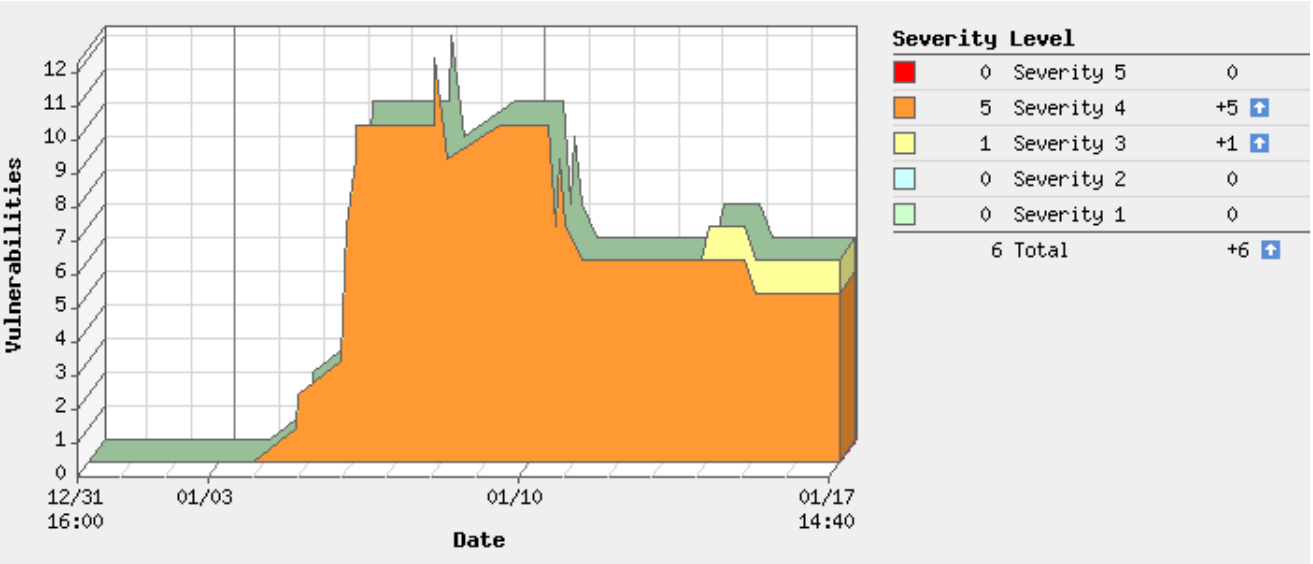

## Vulnerabilities by Severity



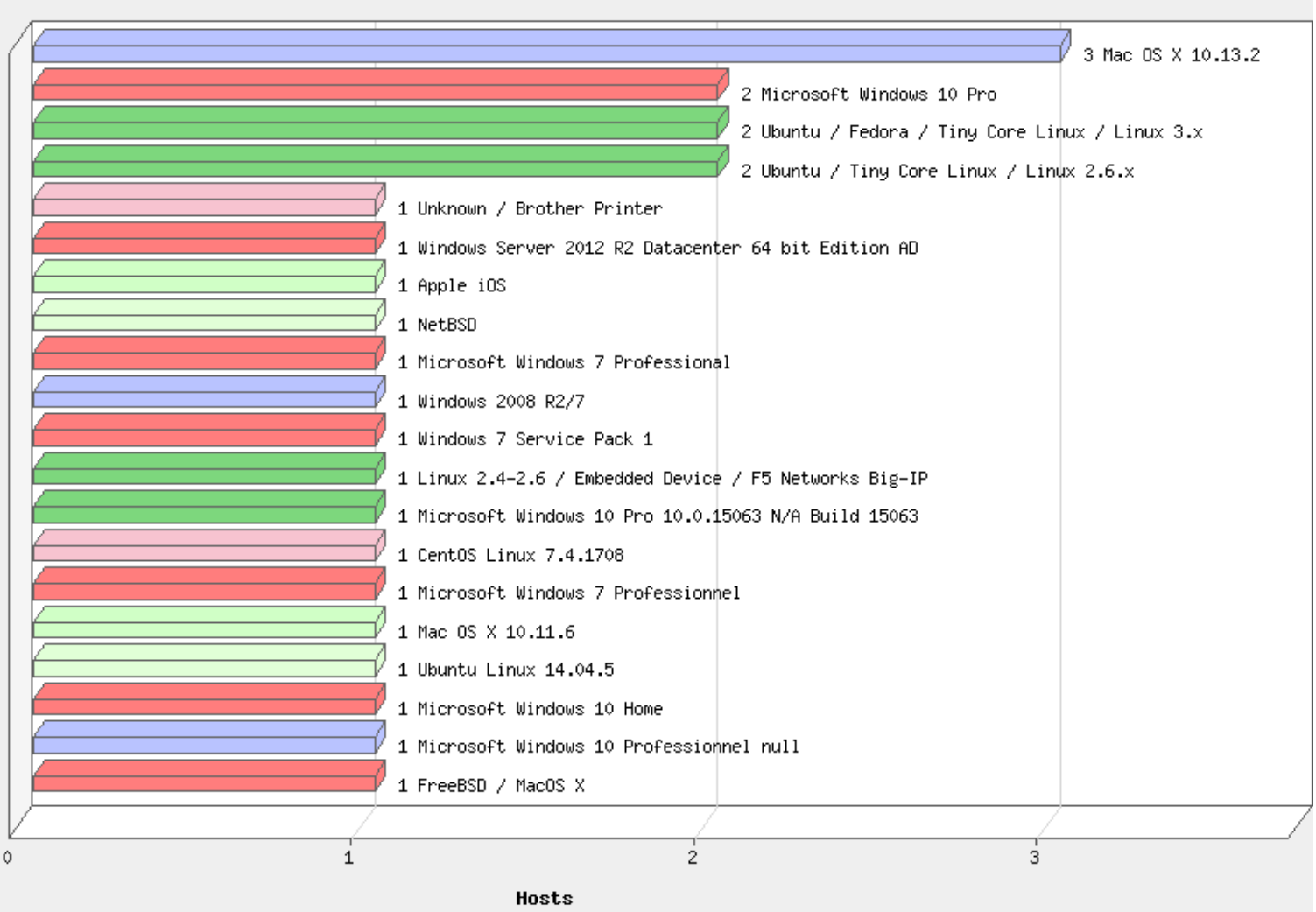
## Information Gathered by Severity




## Vulnerabilities by Severity over Time



## Operating Systems Detected




## Detailed Results

192.168.0.10 (sv-win12-dc01.corp.loftsec.com, SV-WIN12-DC01) Windows Server 2012 R2 Datacent...
TAM-MG-192.168.0.0_24 cpe:/o:microsoft:windows_server_2012:r2::x64:

| Host Identification Information | |
|---|---|
| IPs | |
| Asset Id | 11eea725-c0d7-43bd-9187-6de4c03e21d1 |

| Vulnerabilities Total | 3 (0) - | Security Risk | 0.0 |
|---|---|---|---|

by Status

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

by Severity

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 3 | 3 | (0) - |
| Total | 0 | (0) - | - | | 3 | 3 | (0) - |

| 5 Biggest Categories | | | | | | | |
|---|---|---|---|---|---|---|---|
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| SMB / NETBIOS | 0 | (0) - | - | | 2 | 2 | (0) - |
| Hardware | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 3 | 3 | (0) - |

## Information Gathered (3)

### 1 Processor Information for Windows Target System

QID: 43113
Category: Hardware
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/03/2018
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 08/23/2017 at 09:47:05 AM (GMT-0700)
Last Detected: 01/10/2018 at 08:03:28 AM (GMT-0800)
Times Detected: 5

CVSS Environment:
Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

SOLUTION:
n/a

RESULTS:
HKLM\System\CurrentControlSet\Control\Session Manager\Environment

| | | |
|---|---|---|
| PROCESSOR_IDENTIFIER | = | Intel64 Family 6 Model 94 Stepping 3, GenuineIntel |

### 1 Windows Authentication Method

QID: 70028
Category: SMB / NETBIOS
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 12/09/2008
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 08/23/2017 at 09:47:05 AM (GMT-0700)
Last Detected: 01/10/2018 at 08:03:28 AM (GMT-0800)
Times Detected: 5

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
N/A

RESULTS:

| | |
|---|---|
| User Name | administrator |
| Domain | corp.loftsec.com |
| Authentication Scheme | NTLMSSP v2 |
| Security | User-based |
| SMBv1 Signing | Enabled |
| Discovery Method | Login credentials provided by user |
| CIFS Signing | default |
| Authentication Record | TAM-MG-SV-WIN12-DC01 |
| CIFS Version | SMB v3.0.2 |

 1 Windows Authentication Method for User-Provided Credentials

| | |
|---|---|
| QID: | 70053 |
| Category: | SMB / NETBIOS |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 11/05/2009 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: 08/23/2017 at 09:47:05 AM (GMT-0700)
Last Detected: 01/10/2018 at 08:03:28 AM (GMT-0800)
Times Detected: 5

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
N/A

RESULTS:

| | |
|---|---|
| User Name | administrator |
| Domain | corp.loftsec.com |
| Authentication Scheme | NTLMSSP v2 |

| | |
|---|---|
| Security | User-based |
| SMBv1 Signing | Enabled |
| Authentication Record | TAM-MG-SV-WIN12-DC01 |

## 192.168.0.11 (one-pc, ONE-PC) Windows 7 Service Pack 1
## MKA_Home_Network

| Host Identification Information |
|---|
| IPs |
| Asset Id |

| Vulnerabilities Total | 1 (0) - | Security Risk | 0.0 |
|---|---|---|---|

| by Status | | | |
|---|---|---|---|
| Status | Confirmed | Potential | Total |
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

| by Severity | | | | | | | |
|---|---|---|---|---|---|---|---|
| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

| 5 Biggest Categories | | | | | | | |
|---|---|---|---|---|---|---|---|
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| SMB / NETBIOS | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

## Information Gathered (1)

1 Windows Authentication Method

| | |
|---|---|
| QID: | 70028 |
| Category: | SMB / NETBIOS |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 12/09/2008 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: 01/04/2018 at 08:38:19 AM (GMT-0800)
Last Detected: 01/11/2018 at 12:24:55 AM (GMT-0800)
Times Detected: 5

CVSS Environment:

Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

SOLUTION:
N/A

RESULTS:

| | |
|---|---|
| User Name | (none) |
| Domain | (none) |
| Authentication Scheme | NULL session |
| Security | User-based |
| SMBv1 Signing | Disabled |
| Discovery Method | NULL session, no valid login credentials provided or found |
| CIFS Signing | default |
| CIFS Version | SMB v2.1 |

## 192.168.0.14 (-, HPC4346B088A95) Unknown / Brother Printer
## MKA_Home_Network

| Host Identification Information |
|---|
| IPs |
| Asset Id |

| Vulnerabilities Total | 1 (0) - | Security Risk | 0.0 |
|---|---|---|---|

by Status

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

by Severity

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

5 Biggest Categories

| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| SMB / NETBIOS | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

## Information Gathered (1)

1 Windows Authentication Method

QID: 70028
Category: SMB / NETBIOS
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 12/09/2008
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 01/04/2018 at 09:17:39 AM (GMT-0800)
Last Detected: 01/04/2018 at 09:17:39 AM (GMT-0800)
Times Detected: 1

CVSS Environment:
Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

SOLUTION:
N/A

RESULTS:

| | |
|---|---|
| User Name | (none) |
| Domain | (none) |
| Authentication Scheme | NULL session |
| Security | User-based |
| SMBv1 Signing | Disabled |
| Discovery Method | NULL session, no valid login credentials provided or found |
| CIFS Signing | default |
| CIFS Version | SMB v1 NT LM 0.12 |

## 192.168.1.1 (-, -) Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP
## MCW - Home Network

| Host Identification Information |
|---|
| IPs |
| Asset Id |

| Vulnerabilities Total | 1 (0) - | Security Risk | 0.0 |
|---|---|---|---|

by Status

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

by Severity

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

| 5 Biggest Categories | | | | | | | |
|---|---|---|---|---|---|---|---|
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| Security Policy | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

## Information Gathered (1)

1 Unix Authentication Not Attempted

QID: 105297
Category: Security Policy
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 04/20/2006
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 01/12/2018 at 07:11:50 AM (GMT-0800)
Last Detected: 01/12/2018 at 07:11:50 AM (GMT-0800)
Times Detected: 1

CVSS Environment:
- Asset Group: -
- Collateral Damage Potential: -
- Target Distribution: -
- Confidentiality Requirement: -
- Integrity Requirement: -
- Availability Requirement: -

SOLUTION:
To allow Unix authentication on this host, include the host's IP address in a Unix authentication record.

RESULTS:
No results available

## 101298mbp15.home.private (192.168.1.136, 101298MBP15) FreeBSD / MacOS X
## MCW - Home Network

| Host Identification Information |
|---|
| IPs |
| Asset Id |

| Vulnerabilities Total | 1 (0) - | Security Risk | 0.0 |
|---|---|---|---|

| by Status | | | |
|---|---|---|---|
| Status | Confirmed | Potential | Total |
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

| by Severity | | | | | | | |
|---|---|---|---|---|---|---|---|
| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

| 5 Biggest Categories | | | | | | | |
|---|---|---|---|---|---|---|---|
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| Security Policy | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

## Information Gathered (1)

1 Unix Authentication Failed

QID: 105053
Category: Security Policy
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/12/2005
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 04/17/2017 at 12:13:53 PM (GMT-0700)
Last Detected: 01/12/2018 at 07:10:29 AM (GMT-0800)
Times Detected: 2

CVSS Environment:

Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

SOLUTION:
Verify that the authentication credentials defined in the Unix authentication record are valid for this host. For Unix authentication using private keys, verify that the host contains corresponding public keys. Also verify that a command line daemon service on the host permits network login attempts.

RESULTS:

| Service | SSH |
|---|---|
| User Name | qualys |
| Authentication Record | MCW - UNIX Auth - qualys + AT |

| Diagnostics | Start time: Fri 12 Jan 2018 03:07:14 PM GMT |
|---|---|
| +0:00:00 | SSH: Authentication mode 'none' rejected by target with a 'failure' response code |
| +0:00:00 | SSH: This is expected behavior for the 'none' authentication mode and does not indicate an error |
| +0:00:02 | SSH: Authentication mode 'password' rejected by target with a 'failure' response code |
| +0:00:02 | SSH: This usually means that the credentials were incorrect |
| +0:02:00 | SSH: Target closed the connection |
| +0:02:00 | SSH: Error $22260005 (Received end-of-file on SSH connection) (diag=4) |

## FREEBOX (192.168.0.254, -)

Ubuntu / Fedora / Tiny Core Linux / Linux 3.x

MKA_Home_Network

| Host Identification Information |
|---|
| IPs |
| Asset Id |

| Vulnerabilities Total | 2 (0) - | Security Risk | 0.0 |
|---|---|---|---|

| by Status | | | |
|---|---|---|---|
| Status | Confirmed | Potential | Total |
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

| by Severity | | | | | | | |
|---|---|---|---|---|---|---|---|
| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 2 | 2 | (0) - |
| Total | 0 | (0) - | - | | 2 | 2 | (0) - |

| 5 Biggest Categories | | | | | | | |
|---|---|---|---|---|---|---|---|
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| SMB / NETBIOS | 0 | (0) - | - | | 2 | 2 | (0) - |
| Total | 0 | (0) - | - | | 2 | 2 | (0) - |

## Information Gathered (2)

1 Windows Authentication Method

| | |
|---|---|
| QID: | 70028 |
| Category: | SMB / NETBIOS |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 12/09/2008 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: 11/10/2017 at 12:11:08 PM (GMT-0800)
Last Detected: 01/11/2018 at 12:33:51 AM (GMT-0800)
Times Detected: 6

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
N/A

RESULTS:

| | |
|---|---|
| User Name | (none) |
| Domain | (none) |
| Authentication Scheme | NULL session |
| Security | User-based |
| SMBv1 Signing | Disabled |
| Discovery Method | NULL session,  no valid login credentials provided or found |
| CIFS Signing | default |
| CIFS Version | SMB v1 NT LM 0.12 |

 1 SMB Shares Readable Without Authentication

| | |
|---|---|
| QID: | 70062 |
| Category: | SMB / NETBIOS |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 06/25/2013 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: 11/10/2017 at 12:11:08 PM (GMT-0800)
Last Detected: 01/11/2018 at 12:33:51 AM (GMT-0800)
Times Detected: 6

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
Remove any shares which are not required, or configure the shares to disallow anonymous access or access from a guest user without a password.

RESULTS:

| Share | Comment | Access method |
|---|---|---|
| Disque dur | AutoShare of fbxhdiskd partition 2 | Anonymous access |

| Host Identification Information |
|---|
| IPs |
| Asset Id |

| Vulnerabilities Total | 1 (0) - | Security Risk | 0.0 |
|---|---|---|---|

| by Status | | | |
|---|---|---|---|
| Status | Confirmed | Potential | Total |
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

| by Severity | | | | | | | |
|---|---|---|---|---|---|---|---|
| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

| 5 Biggest Categories | | | | | | | |
|---|---|---|---|---|---|---|---|
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| SMB / NETBIOS | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

## Information Gathered (1)

1 Windows Authentication Method

QID: 70028
Category: SMB / NETBIOS
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 12/09/2008
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 11/10/2017 at 12:07:19 PM (GMT-0800)
Last Detected: 01/11/2018 at 12:30:16 AM (GMT-0800)
Times Detected: 6

CVSS Environment:
- Asset Group: -
- Collateral Damage Potential: -
- Target Distribution: -
- Confidentiality Requirement: -
- Integrity Requirement: -
- Availability Requirement: -

SOLUTION:
N/A

RESULTS:

| | |
|---|---|
| User Name | (none) |
| Domain | (none) |
| Authentication Scheme | NULL session |
| Security | User-based |
| SMBv1 Signing | Disabled |
| Discovery Method | NULL session, no valid login credentials provided or found |
| CIFS Signing | default |

## 10.0.204.236 (101834-t450, 101834-T450) Microsoft Windows 10 Pro
## Global Default Network

| Host Identification Information | |
|---|---|
| IPs | |
| Asset Id | a9c72af4-0005-4732-89fa-448ae0d03ef2 |

| Vulnerabilities Total | 2 (0) - | Security Risk | 0.0 |
|---|---|---|---|

by Status

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 4 | - | 4 |
| Changed | 4 | - | 4 |

by Severity

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 2 | 2 | (0) - |
| Total | 0 | (0) - | - | | 2 | 2 | (0) - |

5 Biggest Categories

| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| Hardware | 0 | (0) - | - | | 2 | 2 | (0) - |
| Total | 0 | (0) - | - | | 2 | 2 | (0) - |

## Vulnerabilities (4)

4 Microsoft Windows Security Update (ADV180002) (Spectre/Meltdown) CVSS: - CVSS3: 4.9 Fixed

| | | | |
|---|---|---|---|
| QID: | 91423 | CVSS Base: | 4.7 |
| Category: | Windows | CVSS Temporal: | 3.5 |
| CVE ID: | CVE-2018-0741, CVE-2018-0743, CVE-2018-0744, CVE-2018-0745, CVE-2018-0746, CVE-2018-0747, CVE-2018-0748, CVE-2018-0749, CVE-2018-0750, CVE-2018-0751, CVE-2018-0752, CVE-2018-0753, CVE-2018-0754, CVE-2018-0788, CVE-2017-5753, CVE-2017-5715, CVE-2017-5754 | | |
| Vendor Reference: | KB4056891, KB4056888, KB4056890, KB4056892, KB4056893, KB4056897, KB4056898, KB4056899, ADV180002, KB4056613, KB4056759, KB4056942, KB4056941, KB4056944 | | |
| Bugtraq ID: | 102371, 102378, 102376, 102349, 102350, 102351, 102353, 102365, 102366, 102354, 102355, 102357, 102359, 102360, 102361, 102362, 102364 | | |

| | | | |
|---|---|---|---|
| Service Modified: | 01/16/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.9 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Closed/Fixed | | |

First Detected: 01/06/2018 at 11:05:56 AM (GMT-0800)

Last Detected: 01/07/2018 at 08:16:10 PM (GMT-0800)

Times Detected: 5

Last Fixed: 01/08/2018 at 06:26:58 PM (GMT-0800)

First Reopened: N/A

Last Reopened: N/A

Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

Customers are advised to refer to ADV180002 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002) for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
kb4056892: Windows (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056892)
KB4056888 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056888)
KB4056890 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056890)
KB4056891 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056891)
KB4056893 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056893)
KB4056897 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056897)
KB4056898 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056898)
KB4056899 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056890)

RESULTS:

KB4056892 is not installed
%windir%\system32\ntdll.dll Version is 10.0.16299.64

4 Mozilla Firefox Spectre Vulnerability (mfsa2018-01)(Spectre) CVSS: - CVSS3: 4.9 Fixed

| | | | |
|---|---|---|---|
| QID: | 370712 | CVSS Base: | 4.7 |
| Category: | Local | CVSS Temporal: | 3.5 |
| CVE ID: | CVE-2017-5753, CVE-2017-5715 | | |
| Vendor Reference: | mfsa2018-01 | | |
| Bugtraq ID: | 102371, 102376 | | |
| Service Modified: | 01/05/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.9 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Closed/Fixed | | |

First Detected: 01/06/2018 at 11:05:56 AM (GMT-0800)

Last Detected: 01/11/2018 at 08:50:55 AM (GMT-0800)

Times Detected: 11

Last Fixed: 01/11/2018 at 07:00:05 PM (GMT-0800)

First Reopened: N/A

Last Reopened: N/A

Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

The vendor has issued a fix (57.0.4).
Refer to MFSA 2018-01 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2018-01: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/)
MFSA 2018-01: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/)

RESULTS:

C:\Program Files (x86)\Mozilla Firefox\firefox.exe Version is 57.0.2.0

4 Microsoft Internet Explorer Security Update for January 2018 (ADV180002) (Spectre/Meltdown) CVSS: - CVSS3: 4.9 Fixed

| | | | |
|---|---|---|---|
| QID: | 100326 | CVSS Base: | 4.7 |
| Category: | Internet Explorer | CVSS Temporal: | 3.5 |
| CVE ID: | CVE-2017-5753, CVE-2017-5754, CVE-2017-5715, CVE-2018-0762, CVE-2018-0772 | | |
| Vendor Reference: | ADV180002, KB4056568, KB4056893, KB4056890, KB4056891, KB4056892, KB4056888, KB4056894, KB4056895, KB4056896 | | |
| Bugtraq ID: | 102371, 102376, 102378, 102408, 102409 | | |
| Service Modified: | 01/10/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.9 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Closed/Fixed | | |

First Detected: 01/06/2018 at 11:05:56 AM (GMT-0800)

Last Detected: 01/07/2018 at 08:16:10 PM (GMT-0800)

Times Detected: 5

Last Fixed: 01/08/2018 at 06:26:58 PM (GMT-0800)

First Reopened: N/A

Last Reopened: N/A

Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

For more information, Customers are advised to refer the Security Update Guide. (https://portal.msrc.microsoft.com/en-us/security-guidance)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Microsoft Security Update Guide (https://portal.msrc.microsoft.com/en-us/security-guidance)

RESULTS:

%programfiles%\Internet Explorer\iexplore.exe found
%programfiles(x86)%\Internet Explorer\iexplore.exe found
KB4056892 is not installed
%windir%\System32\mshtml.dll Version is 11.0.16299.125

HKLM\Software\Microsoft\Internet Explorer Version = 9.11.16299.0

4 Microsoft Edge Security Update for January 2018 (ADV180002) (Spectre/Meltdown) CVSS: - CVSS3: 4.9 Fixed

| | | | |
|---|---|---|---|
| QID: | 91425 | CVSS Base: | 7.6 |
| Category: | Windows | CVSS Temporal: | 5.6 |
| CVE ID: | CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, CVE-2018-0780, CVE-2018-0781, CVE-2018-0800, CVE-2018-0803, CVE-2018-0758, CVE-2018-0762, CVE-2018-0766, CVE-2018-0767, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2017-5753, CVE-2017-5754, CVE-2017-5715 | | |
| Vendor Reference: | KB4056892, KB4056888, KB4056890, KB4056893, KB4056891, ADV180002 | | |
| Bugtraq ID: | 102371, 102376, 102378, 102405, 102408, 102388, 102393, 102395, 102396, 102397, 102409, 102398, 102399, 102400, 102401, 102402, 102403, 102389, 102404, 102392, 102384 | | |
| Service Modified: | 01/09/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.9 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Closed/Fixed | | |

First Detected: 01/06/2018 at 11:05:56 AM (GMT-0800)

Last Detected: 01/07/2018 at 08:16:10 PM (GMT-0800)

Times Detected: 5

Last Fixed: 01/08/2018 at 06:26:58 PM (GMT-0800)

First Reopened: N/A

Last Reopened: N/A

Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

For more information, customers are advised to refer the Security Update Guide. (https://portal.msrc.microsoft.com/en-us/security-guidance)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Microsoft Security Update Guide (https://portal.msrc.microsoft.com/en-us/security-guidance)

RESULTS:

KB4056892 is not installed
%windir%\System32\edgehtml.dll Version is 11.0.16299.125

## Information Gathered (2)

1 Processor Information for Windows Target System

| | |
|---|---|
| QID: | 43113 |
| Category: | Hardware |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 01/03/2018 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: 10/17/2017 at 06:52:58 PM (GMT-0700)
Last Detected: 01/17/2018 at 10:45:30 AM (GMT-0800)
Times Detected: 194

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
n/a

RESULTS:

| HKLM\System\CurrentControlSet\Control\Session Manager\Environment | | |
|---|---|---|
| PROCESSOR_IDENTIFIER | = | Intel64 Family 6 Model 61 Stepping 4, GenuineIntel |

 1 Processor And BIOS Information Overview On Windows

| | |
|---|---|
| QID: | 43567 |
| Category: | Hardware |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 01/10/2018 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: 01/17/2018 at 10:45:30 AM (GMT-0800)
Last Detected: 01/17/2018 at 10:45:30 AM (GMT-0800)
Times Detected: 1

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
N/A

RESULTS:

| | | |
|---|---|---|
| PROCESSOR_IDENTIFIER | = | Intel64 Family 6 Model 61 Stepping 4, GenuineIntel |
| HKLM\Hardware\Description\System\BIOS | | |
| BIOSVendor | = | LENOVO |
| HKLM\Hardware\Description\System\BIOS | | |
| BIOSVersion | = | JBET67WW (1.31 ) |
| | | |
| SystemProductName | = | 20BV000DUS |
| ComputerHardwareId | = | {679d5d77-7828-53ed-9f66-e3ede29d9de1} |

| | |
|---|---|
| BIOSReleaseDate | = 12/14/2017 |
| BIOSVersion | = JBET67WW (1.31 ) |
| InformationSource | = 1 |
| SystemManufacturer | = LENOVO |
| ComputerHardwareIds | = |

## 192.168.0.31 (one-pc, ONE-PC) — Microsoft Windows 7 Professionnel
## Global Default Network

| Host Identification Information | |
|---|---|
| IPs | |
| Asset Id | 56d4ff15-0376-4775-b4bd-c6628dd733fb |

| Vulnerabilities Total | 2 (0) - | Security Risk | 0.0 |
|---|---|---|---|

by Status

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 2 | - | 2 |
| Changed | 2 | - | 2 |

by Severity

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 2 | 2 | (0) - |
| Total | 0 | (0) - | - | | 2 | 2 | (0) - |

5 Biggest Categories

| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| Windows | 0 | (0) - | - | | 1 | 1 | (0) - |
| Hardware | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 2 | 2 | (0) - |

## Vulnerabilities (2)

4 Microsoft Windows Security Update (ADV180002) (Spectre/Meltdown) CVSS: - CVSS3: 4.9 Fixed

| | | | |
|---|---|---|---|
| QID: | 91423 | CVSS Base: | 4.7 |
| Category: | Windows | CVSS Temporal: | 3.5 |
| CVE ID: | CVE-2018-0741, CVE-2018-0743, CVE-2018-0744, CVE-2018-0745, CVE-2018-0746, CVE-2018-0747, CVE-2018-0748, CVE-2018-0749, CVE-2018-0750, CVE-2018-0751, CVE-2018-0752, CVE-2018-0753, CVE-2018-0754, CVE-2018-0788, CVE-2017-5753, CVE-2017-5715, CVE-2017-5754 | | |
| Vendor Reference: | KB4056891, KB4056888, KB4056890, KB4056892, KB4056893, KB4056897, KB4056898, KB4056899, ADV180002, KB4056613, KB4056759, KB4056942, KB4056941, KB4056944 | | |
| Bugtraq ID: | 102371, 102378, 102376, 102349, 102350, 102351, 102353, 102365, 102366, 102354, 102355, 102357, 102359, 102360, 102361, 102362, 102364 | | |
| Service Modified: | 01/16/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.9 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |

Ticket State: Closed/Fixed

First Detected: 01/06/2018 at 04:33:52 PM (GMT-0800)
Last Detected: 01/07/2018 at 05:29:45 PM (GMT-0800)
Times Detected: 2
Last Fixed: 01/11/2018 at 10:15:29 AM (GMT-0800)

First Reopened: N/A
Last Reopened: N/A
Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
Customers are advised to refer to ADV180002 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002) for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
kb4056892: Windows (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056892)
KB4056888 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056888)
KB4056890 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056890)
KB4056891 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056891)
KB4056893 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056893)
KB4056897 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056897)
KB4056898 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056898)
KB4056899 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056890)

RESULTS:
KB4056897 is not installed
%windir%\system32\ntdll.dll Version is 6.1.7601.23915

 4 Microsoft Internet Explorer Security Update for January 2018 (ADV180002) (Spectre/Meltdown) CVSS: - CVSS3: 4.9 Fixed

| | | | |
|---|---|---|---|
| QID: | 100326 | CVSS Base: | 4.7 |
| Category: | Internet Explorer | CVSS Temporal: | 3.5 |
| CVE ID: | CVE-2017-5753, CVE-2017-5754, CVE-2017-5715, CVE-2018-0762, CVE-2018-0772 | | |
| Vendor Reference: | ADV180002, KB4056568, KB4056893, KB4056890, KB4056891, KB4056892, KB4056888, KB4056894, KB4056895, KB4056896 | | |
| Bugtraq ID: | 102371, 102376, 102378, 102408, 102409 | | |
| Service Modified: | 01/10/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.9 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Closed/Fixed | | |

First Detected: 01/06/2018 at 04:33:52 PM (GMT-0800)
Last Detected: 01/07/2018 at 05:29:45 PM (GMT-0800)
Times Detected: 2
Last Fixed: 01/11/2018 at 10:15:29 AM (GMT-0800)

First Reopened: N/A
Last Reopened: N/A
Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
For more information, Customers are advised to refer the Security Update Guide. (https://portal.msrc.microsoft.com/en-us/security-guidance)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Microsoft Security Update Guide (https://portal.msrc.microsoft.com/en-us/security-guidance)

RESULTS:

%programfiles%\Internet Explorer\iexplore.exe found
%programfiles(x86)%\Internet Explorer\iexplore.exe found
KB4056568 is not installed
%windir%\System32\mshtml.dll Version is 11.0.9600.18860
HKLM\Software\Microsoft\Internet Explorer Version = 9.11.9600.18860

## Information Gathered (2)

### 1 Processor Information for Windows Target System

| | |
|---|---|
| QID: | 43113 |
| Category: | Hardware |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 01/03/2018 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: 01/06/2018 at 04:33:52 PM (GMT-0800)
Last Detected: 01/14/2018 at 11:38:11 AM (GMT-0800)
Times Detected: 4

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
n/a

RESULTS:
HKLM\System\CurrentControlSet\Control\Session Manager\Environment

| | | |
|---|---|---|
| PROCESSOR_IDENTIFIER | = | Intel64 Family 6 Model 69 Stepping 1, GenuineIntel |

### 1 Microsoft Windows Network Level Authentication Disabled

| | |
|---|---|
| QID: | 90788 |
| Category: | Windows |
| CVE ID: | - |

Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/01/2013
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 01/06/2018 at 04:33:52 PM (GMT-0800)
Last Detected: 01/14/2018 at 11:38:11 AM (GMT-0800)
Times Detected: 4

CVSS Environment:

Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

SOLUTION:
See Microsoft Knowledge Base Article 2671387 (http://support.microsoft.com/kb/2671387) to use the automated Microsoft Fix it solution to enable this feature.
As a precaution, always test in a QA or rehearsal environment before rolling out to production.
Note: Client computers that do not support Credential Security Support Provider (CredSSP) protocol will not be able to access servers protected with Network Level Authentication. Windows XP does not support the CredSSP protocol by default.

RESULTS:
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\EH-Tcp UserAuthentication = 2
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp UserAuthentication = 0

## 192.168.1.5 (nuc.home.private, -)
## Global Default Network

## CentOS Linux 7.4.1708
## cpe:/o:centos:centos_linux:7.4.1708:::

| Host Identification Information | |
|---|---|
| IPs | 192.168.122.1, 192.168.1.5, fe80::df35:b1d8:b4ad:331a |
| Asset Id | 58f5129b-00c3-0002-7e4e-000c29691706 |

| Vulnerabilities Total | 1 (+1) | Security Risk | 4.0 |
|---|---|---|---|

by Status

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 0 | - | 0 |
| Active | 1 | - | 1 |
| Re-Opened | 0 | - | 0 |
| Total | 1 | - | 1 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

by Severity

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 1 | (+1) | - | | 0 | 1 | (+1) |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 0 | 0 | (0) - |
| Total | 1 | (+1) | - | | 0 | 1 | (+1) |

| 5 Biggest Categories | | | | | | | |
|---|---|---|---|---|---|---|---|
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| CentOS | 1 | (+1) | - | | 0 | 1 | (+1) |
| Total | 1 | (+1) | - | | 0 | 1 | (+1) |

## Vulnerabilities (1)

4 CentOS Security Update for kernel (CESA-2018:0007) (Spectre/Meltdown) CVSS: - CVSS3: 5.1 Active

| | | | |
|---|---|---|---|
| QID: | 256345 | CVSS Base: | 4.7 |
| Category: | CentOS | CVSS Temporal: | 3.7 |
| CVE ID: | CVE-2017-5715, CVE-2017-5753, CVE-2017-5754 | | |
| Vendor Reference: | CESA-2018:0007 centos 7 | | |
| Bugtraq ID: | 102376, 102371, 102378 | | |
| Service Modified: | 01/05/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 5.1 |
| Edited: | No | | |
| PCI Vuln: | No | | |
| Ticket State: | Open | | |

First Detected: 01/06/2018 at 08:03:47 AM (GMT-0800)

Last Detected: 01/17/2018 at 04:33:50 AM (GMT-0800)

Times Detected: 31

Last Fixed: N/A

First Reopened: N/A

Last Reopened: N/A

Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

To resolve this issue, upgrade to the latest packages which contain a patch.
Refer to CentOS advisory centos 7 (https://lists.centos.org/pipermail/centos-announce/2018-January/022696.html) for updates and patch information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
CESA-2018:0007: centos 7 (https://lists.centos.org/pipermail/centos-announce/2018-January/022696.html)

RESULTS:

kernel 3.10.0-693.2.2.el7 3.10.0-693.11.6.el7
kernel 3.10.0-693.11.1.el7 3.10.0-693.11.6.el7
kernel 3.10.0-514.26.2.el7 3.10.0-693.11.6.el7
kernel 3.10.0-693.5.2.el7 3.10.0-693.11.6.el7
kernel-devel 3.10.0-693.11.1.el7 3.10.0-693.11.6.el7
kernel-devel 3.10.0-693.2.2.el7 3.10.0-693.11.6.el7
kernel-devel 3.10.0-514.26.2.el7 3.10.0-693.11.6.el7
kernel-devel 3.10.0-693.5.2.el7 3.10.0-693.11.6.el7

## 192.168.1.18 (gamingmonster, GAMINGMONSTER) Microsoft Windows 10 Pro 10.0.15063 N/A Build ...
## Global Default Network

| Host Identification Information | |
|---|---|
| IPs | |
| Asset Id | c152c6e6-3deb-4bf7-8829-26f986e5d9d9 |

| Vulnerabilities Total | 2 (+1) | Security Risk | 4.0 |
|---|---|---|---|

**by Status**

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 1 | - | 1 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 1 | - | 1 |
| Fixed | 0 | - | 0 |
| Changed | 1 | - | 1 |

**by Severity**

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 1 | (+1) | - | | 0 | 1 | (+1) |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 1 | (+1) | - | | 1 | 2 | (+1) |

**5 Biggest Categories**

| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| Windows | 1 | (+1) | - | | 0 | 1 | (+1) |
| Hardware | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 1 | (+1) | - | | 1 | 2 | (+1) |

## Vulnerabilities (1)

4 Microsoft Edge Security Update for January 2018 (ADV180002) (Spectre/Meltdown) CVSS: - CVSS3: 4.9 New

| | | | |
|---|---|---|---|
| QID: | 91425 | CVSS Base: | 7.6 |
| Category: | Windows | CVSS Temporal: | 5.6 |
| CVE ID: | CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, CVE-2018-0780, CVE-2018-0781, CVE-2018-0800, CVE-2018-0803, CVE-2018-0758, CVE-2018-0762, CVE-2018-0766, CVE-2018-0767, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2017-5753, CVE-2017-5754, CVE-2017-5715 | | |
| Vendor Reference: | KB4056892, KB4056888, KB4056890, KB4056893, KB4056891, ADV180002 | | |
| Bugtraq ID: | 102371, 102376, 102378, 102405, 102408, 102388, 102393, 102395, 102396, 102397, 102409, 102398, 102399, 102400, 102401, 102402, 102403, 102389, 102404, 102392, 102384 | | |
| Service Modified: | 01/09/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.9 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Open | | |

First Detected: 01/05/2018 at 08:18:46 AM (GMT-0800)
Last Detected: 01/05/2018 at 08:18:46 AM (GMT-0800)
Times Detected: 1
Last Fixed: N/A

First Reopened: N/A
Last Reopened: N/A
Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
For more information, customers are advised to refer the Security Update Guide. (https://portal.msrc.microsoft.com/en-us/security-guidance)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Microsoft Security Update Guide (https://portal.msrc.microsoft.com/en-us/security-guidance)

RESULTS:

KB4056891 is not installed
%windir%\System32\edgehtml.dll Version is 11.0.15063.786

## Information Gathered (1)

1 Processor Information for Windows Target System

| | |
|---|---|
| QID: | 43113 |
| Category: | Hardware |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 01/03/2018 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: N/A
Last Detected: 01/05/2018 at 08:18:46 AM (GMT-0800)
Times Detected: 209

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
n/a

RESULTS:
HKLM\System\CurrentControlSet\Control\Session Manager\Environment

| | | |
|---|---|---|
| PROCESSOR_IDENTIFIER | = | Intel64 Family 6 Model 79 Stepping 1, GenuineIntel |

| Host Identification Information | |
|---|---|
| IPs | 192.168.1.125, 10.0.204.230, fe80::5153:5a22:275b:8422, fe80::6203:8ff:fe9d:8cf2, fe80::1, fe80::c0cb:f4ff:feb9:6bd9 |
| Asset Id | 2e824737-cd6b-4577-b0a0-5db351b25235 |

| Vulnerabilities Total | 2 (+1) | Security Risk | 4.0 |
|---|---|---|---|

by Status

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 0 | - | 0 |
| Active | 1 | - | 1 |
| Re-Opened | 0 | - | 0 |
| Total | 1 | - | 1 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

by Severity

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 1 | (+1) | - | | 0 | 1 | (+1) |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 1 | (+1) | - | | 1 | 2 | (+1) |

5 Biggest Categories

| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| Local | 1 | (+1) | - | | 0 | 1 | (+1) |
| Hardware | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 1 | (+1) | - | | 1 | 2 | (+1) |

## Vulnerabilities (1)

4 Apple macOS Security Update for High Sierra, Sierra and El Capitan Not Installed (Meltdown) CVSS: - CVSS3: 5.1 Active

| | | | |
|---|---|---|---|
| QID: | 370710 | CVSS Base: | 4.7 |
| Category: | Local | CVSS Temporal: | 3.7 |
| CVE ID: | CVE-2017-5754 | | |
| Vendor Reference: | HT208331 | | |
| Bugtraq ID: | 102378, 102097, 102099, 102100, 101981, 100515, 100872 | | |
| Service Modified: | 01/08/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 5.1 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Open | | |

First Detected: 01/09/2018 at 10:23:25 PM (GMT-0800)
Last Detected: 01/17/2018 at 04:32:36 AM (GMT-0800)
Times Detected: 8
Last Fixed: N/A

First Reopened: N/A
Last Reopened: N/A
Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
The update can be downloaded and installed via Apple Downloads (http://support.apple.com/downloads/).
For more information regarding the update can be found at HT208331 (https://support.apple.com/en-in/HT208331).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
HT208331: macOS High Sierra (https://support.apple.com/en-in/HT208331)

RESULTS:

Security Update 2017-005 is missing.
2017-002 is missing.

## Information Gathered (1)

 1 Apple Macintosh Processor Architecture

| | |
|---|---|
| QID: | 43110 |
| Category: | Hardware |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 01/03/2018 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: 04/04/2017 at 12:02:03 PM (GMT-0700)
Last Detected: 01/17/2018 at 04:32:36 AM (GMT-0800)
Times Detected: 205

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
N/A

RESULTS:

Processor Name: Intel Core i7
Processor Speed: 2.3 GHz
Number of Processors: 1
Total Number of Cores: 4
L2 Cache (per Core): 256 KB

| Host Identification Information | |
|---|---|
| IPs | |
| Asset Id | 40898c7a-8b72-4046-9644-154478a48e91 |

| Vulnerabilities Total | 1 (0) - | Security Risk | 0.0 |
|---|---|---|---|

| by Status | | | |
|---|---|---|---|
| Status | Confirmed | Potential | Total |
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

| by Severity | | | | | | | |
|---|---|---|---|---|---|---|---|
| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

| 5 Biggest Categories | | | | | | | |
|---|---|---|---|---|---|---|---|
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| Hardware | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

## Information Gathered (1)

1 Apple Macintosh Processor Architecture

QID: 43110
Category: Hardware
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/03/2018
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 09/11/2017 at 11:01:03 AM (GMT-0700)
Last Detected: 01/08/2018 at 10:54:04 AM (GMT-0800)
Times Detected: 185

CVSS Environment:
Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

SOLUTION:
N/A

RESULTS:

Processor Name: Intel Core i7
Processor Speed: 2.5 GHz
Number of Processors: 1
Total Number of Cores: 4
L2 Cache (per Core): 256 KB

## 192.168.1.136 (101298mbp15.home.private, 101298MBP15) Mac OS X 10.13.2
## Global Default Network

| Host Identification Information | |
|---|---|
| IPs | |
| Asset Id | f3e72bc3-5dd1-460f-8857-fd46f22ca2f7 |

| Vulnerabilities Total | 2 (+1) | Security Risk | 4.0 |
|---|---|---|---|

by Status

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 0 | - | 0 |
| Active | 1 | - | 1 |
| Re-Opened | 0 | - | 0 |
| Total | 1 | - | 1 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

by Severity

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 1 | (+1) | - | | 0 | 1 | (+1) |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 1 | (+1) | - | | 1 | 2 | (+1) |

5 Biggest Categories

| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| Local | 1 | (+1) | - | | 0 | 1 | (+1) |
| Hardware | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 1 | (+1) | - | | 1 | 2 | (+1) |

## Vulnerabilities (1)

4 Apple macOS High Sierra Supplemental Update / Safari 11.0.2 update (Spectre) CVSS: - CVSS3: 5.1 Active

| | | | |
|---|---|---|---|
| QID: | 370716 | CVSS Base: | 4.7 |
| Category: | Local | CVSS Temporal: | 3.7 |
| CVE ID: | CVE-2017-5753, CVE-2017-5715 | | |
| Vendor Reference: | HT208397, HT208403 | | |
| Bugtraq ID: | 102376, 102371 | | |
| Service Modified: | 01/09/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 5.1 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Open | | |

First Detected: 01/11/2018 at 06:39:42 AM (GMT-0800)

Last Detected: 01/17/2018 at 02:21:50 AM (GMT-0800)

Times Detected: 15

Last Fixed: N/A

First Reopened: N/A

Last Reopened: N/A

Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

The update can be downloaded and installed via Apple Downloads (http://support.apple.com/downloads/).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
HT208397: OS X High Sierra (https://support.apple.com/en-us/HT208397)
HT208403: Safari for Mac OS X (https://support.apple.com/en-us/HT208403)

RESULTS:

<key>CFBundleVersion</key>
<string>13604.4.7.1.3</string>

## Information Gathered (1)

1 Apple Macintosh Processor Architecture

| | |
|---|---|
| QID: | 43110 |
| Category: | Hardware |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 01/03/2018 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: N/A

Last Detected: 01/17/2018 at 02:21:50 AM (GMT-0800)

Times Detected: 769

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
N/A

RESULTS:

Processor Name: Intel Core i7

Processor Speed: 2.5 GHz
Number of Processors: 1
Total Number of Cores: 4
L2 Cache (per Core): 256 KB

## 192.168.1.196 (101282-t440, 101282-T440) Microsoft Windows 7 Professional
## Global Default Network

| Host Identification Information | |
|---|---|
| IPs | |
| Asset Id | 054d6d07-ac8e-43d7-9fc4-a08972fa7ba1 |

| Vulnerabilities Total | 2 (0) - | Security Risk | 0.0 |
|---|---|---|---|

**by Status**

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

**by Severity**

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 2 | 2 | (0) - |
| Total | 0 | (0) - | - | | 2 | 2 | (0) - |

**5 Biggest Categories**

| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| Windows | 0 | (0) - | - | | 1 | 1 | (0) - |
| Hardware | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 2 | 2 | (0) - |

## Information Gathered (2)

1 Processor Information for Windows Target System

QID: 43113
Category: Hardware
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/03/2018
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 01/12/2018 at 01:48:59 PM (GMT-0800)
Last Detected: 01/16/2018 at 08:49:18 AM (GMT-0800)
Times Detected: 3

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
n/a

RESULTS:
HKLM\System\CurrentControlSet\Control\Session Manager\Environment

| | | |
|---|---|---|
| PROCESSOR_IDENTIFIER | = | Intel64 Family 6 Model 60 Stepping 3, GenuineIntel |

 1 Microsoft Windows Network Level Authentication Disabled

| | |
|---|---|
| QID: | 90788 |
| Category: | Windows |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 05/01/2013 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: 01/12/2018 at 01:48:59 PM (GMT-0800)
Last Detected: 01/16/2018 at 08:49:18 AM (GMT-0800)
Times Detected: 3

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
See Microsoft Knowledge Base Article 2671387 (http://support.microsoft.com/kb/2671387) to use the automated Microsoft Fix it solution to enable this feature.
As a precaution, always test in a QA or rehearsal environment before rolling out to production.
Note: Client computers that do not support Credential Security Support Provider (CredSSP) protocol will not be able to access servers protected with Network Level Authentication. Windows XP does not support the CredSSP protocol by default.

RESULTS:
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\EH-Tcp UserAuthentication = 2
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp UserAuthentication = 0

| Host Identification Information | |
|---|---|
| IPs | |
| Asset Id | f8e257ee-57d8-4ac1-abc5-a4fe76f10268 |

| Vulnerabilities Total | 1 (0) - | Security Risk | 0.0 |
|---|---|---|---|

| by Status | | | |
|---|---|---|---|
| Status | Confirmed | Potential | Total |
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

| by Severity | | | | | | | |
|---|---|---|---|---|---|---|---|
| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

| 5 Biggest Categories | | | | | | | |
|---|---|---|---|---|---|---|---|
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| Hardware | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

## Information Gathered (1)

1 Processor Information for Windows Target System

QID: 43113
Category: Hardware
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/03/2018
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 04/07/2017 at 06:18:51 PM (GMT-0700)
Last Detected: 01/17/2018 at 04:00:29 AM (GMT-0800)
Times Detected: 274

CVSS Environment:
- Asset Group: -
- Collateral Damage Potential: -
- Target Distribution: -
- Confidentiality Requirement: -
- Integrity Requirement: -
- Availability Requirement: -

SOLUTION:
n/a

RESULTS:

| HKLM\System\CurrentControlSet\Control\Session Manager\Environment | | |
|---|---|---|
| PROCESSOR_IDENTIFIER | = | x86 Family 6 Model 23 Stepping 10, GenuineIntel |

## 192.168.127.1 (lenovox1-100707, LENOVOX1-100707) Microsoft Windows 10 Professionnel null
## Global Default Network

| Host Identification Information | |
|---|---|
| IPs | |
| Asset Id | 527f8c28-8e59-4397-8133-df7a44b80951 |

| Vulnerabilities Total | 1 (0) - | Security Risk | 0.0 |
|---|---|---|---|

| by Status | | | |
|---|---|---|---|
| Status | Confirmed | Potential | Total |
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 0 | - | 0 |
| Changed | 0 | - | 0 |

| by Severity | | | | | | | |
|---|---|---|---|---|---|---|---|
| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

| 5 Biggest Categories | | | | | | | |
|---|---|---|---|---|---|---|---|
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| Hardware | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

## Information Gathered (1)

1 Processor Information for Windows Target System

QID: 43113
Category: Hardware
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/03/2018
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A
Last Detected: 01/14/2018 at 04:03:57 PM (GMT-0800)
Times Detected: 2

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
n/a

RESULTS:
HKLM\System\CurrentControlSet\Control\Session Manager\Environment

| | | |
|---|---|---|
| PROCESSOR_IDENTIFIER | = | Intel64 Family 6 Model 61 Stepping 4, GenuineIntel |

## 192.168.135.128 (ubuntu, -) Ubuntu Linux 14.04.5
## Global Default Network

| Host Identification Information | |
|---|---|
| IPs | 192.168.135.128, fe80::20c:29ff:febd:fc42 |
| Asset Id | cbefd713-8f79-4e9e-b6ce-1ccd8f313b82 |

| Vulnerabilities Total | 1 (+1) | Security Risk | 3.0 |
|---|---|---|---|

by Status

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 1 | - | 1 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 1 | - | 1 |
| Fixed | 0 | - | 0 |
| Changed | 1 | - | 1 |

by Severity

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 1 | (+1) | - | | 0 | 1 | (+1) |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 0 | 0 | (0) - |
| Total | 1 | (+1) | - | | 0 | 1 | (+1) |

5 Biggest Categories

| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| Ubuntu | 1 | (+1) | - | | 0 | 1 | (+1) |
| Total | 1 | (+1) | - | | 0 | 1 | (+1) |

## Vulnerabilities (1)

3 Ubuntu Security Notification for Firefox Vulnerabilities (USN-3516-1) CVSS: - CVSS3: 4.5 New

| | | | |
|---|---|---|---|
| QID: | 197006 | CVSS Base: | 4.7 |
| Category: | Ubuntu | CVSS Temporal: | 3.5 |
| CVE ID: | CVE-2017-5715, CVE-2017-5753, CVE-2017-5754 | | |
| Vendor Reference: | USN-3516-1 | | |

| | | | |
|---|---|---|---|
| Bugtraq ID: | 102376, 102371, 102378 | | |
| Service Modified: | 01/10/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.5 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Open | | |

First Detected: 01/14/2018 at 03:50:52 PM (GMT-0800)

Last Detected: 01/14/2018 at 03:50:52 PM (GMT-0800)

Times Detected: 1

Last Fixed: N/A

First Reopened: N/A

Last Reopened: N/A

Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

Refer to Ubuntu advisory USN-3516-1 (https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-January/004204.html) for affected packages and patching details, or update with your package manager.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
USN-3516-1: 16.04 (Xenial) on src (firefox) (https://launchpad.net/ubuntu/+source/firefox/57.0.4+build1-0ubuntu0.16.04.1)
USN-3516-1: 17.10 (artful) on src (firefox) (https://launchpad.net/ubuntu/+source/firefox/57.0.4+build1-0ubuntu0.17.10.1)
USN-3516-1: 17.04 (zesty) on src (firefox) (https://launchpad.net/ubuntu/+source/firefox/57.0.4+build1-0ubuntu0.17.04.1)
USN-3516-1: 14.04 (Kylin) on src (firefox) (https://launchpad.net/ubuntu/+source/firefox/57.0.4+build1-0ubuntu0.14.04.1)

RESULTS:

firefox 50.1.0+build2-0ubuntu0.14.04.1 57.0.4+build1-0ubuntu0.14.04.1

## 192.168.154.1 (desktop-81s80ep, DESKTOP-81S80EP) Microsoft Windows 10 Pro
## Global Default Network

| Host Identification Information | |
|---|---|
| IPs | |
| Asset Id | 9fff5aa5-cabe-4b53-ad35-38790d8f9572 |

| Vulnerabilities Total | 1 (0) - | Security Risk | 0.0 |
|---|---|---|---|

by Status

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 0 | - | 0 |
| Active | 0 | - | 0 |
| Re-Opened | 0 | - | 0 |
| Total | 0 | - | 0 |
| Fixed | 3 | - | 3 |
| Changed | 3 | - | 3 |

by Severity

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 4 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

| 5 Biggest Categories | | | | | | | |
|---|---|---|---|---|---|---|---|
| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
| Hardware | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 0 | (0) - | - | | 1 | 1 | (0) - |

## Vulnerabilities (3)

4 Microsoft Windows Security Update (ADV180002) (Spectre/Meltdown) CVSS: - CVSS3: 4.9 Fixed

| | | | |
|---|---|---|---|
| QID: | 91423 | CVSS Base: | 4.7 |
| Category: | Windows | CVSS Temporal: | 3.5 |
| CVE ID: | CVE-2018-0741, CVE-2018-0743, CVE-2018-0744, CVE-2018-0745, CVE-2018-0746, CVE-2018-0747, CVE-2018-0748, CVE-2018-0749, CVE-2018-0750, CVE-2018-0751, CVE-2018-0752, CVE-2018-0753, CVE-2018-0754, CVE-2018-0788, CVE-2017-5753, CVE-2017-5715, CVE-2017-5754 | | |
| Vendor Reference: | KB4056891, KB4056888, KB4056890, KB4056892, KB4056893, KB4056897, KB4056898, KB4056899, ADV180002, KB4056613, KB4056759, KB4056942, KB4056941, KB4056944 | | |
| Bugtraq ID: | 102371, 102378, 102376, 102349, 102350, 102351, 102353, 102365, 102366, 102354, 102355, 102357, 102359, 102360, 102361, 102362, 102364 | | |
| Service Modified: | 01/16/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.9 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Closed/Fixed | | |

First Detected: 01/08/2018 at 11:36:44 AM (GMT-0800)

Last Detected: 01/09/2018 at 01:02:56 PM (GMT-0800)

Times Detected: 2

Last Fixed: 01/11/2018 at 04:43:59 AM (GMT-0800)

First Reopened: N/A

Last Reopened: N/A

Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

Customers are advised to refer to ADV180002 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002) for more details pertaining to this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
kb4056892: Windows (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056892)
KB4056888 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056888)
KB4056890 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056890)
KB4056891 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056891)
KB4056893 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056893)
KB4056897 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056897)
KB4056898 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056898)
KB4056899 (http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056890)

RESULTS:

KB4056892 is not installed
%windir%\system32\win32kfull.sys Version is 10.0.16299.125

4 Microsoft Internet Explorer Security Update for January 2018 (ADV180002) (Spectre/Meltdown) CVSS: - CVSS3: 4.9 Fixed

| | | | |
|---|---|---|---|
| QID: | 100326 | CVSS Base: | 4.7 |
| Category: | Internet Explorer | CVSS Temporal: | 3.5 |
| CVE ID: | CVE-2017-5753, CVE-2017-5754, CVE-2017-5715, CVE-2018-0762, CVE-2018-0772 | | |
| Vendor Reference: | ADV180002, KB4056568, KB4056893, KB4056890, KB4056891, KB4056892, KB4056888, KB4056894, KB4056895, KB4056896 | | |
| Bugtraq ID: | 102371, 102376, 102378, 102408, 102409 | | |
| Service Modified: | 01/10/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.9 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Closed/Fixed | | |

First Detected: 01/08/2018 at 11:36:44 AM (GMT-0800)

Last Detected: 01/09/2018 at 01:02:56 PM (GMT-0800)

Times Detected: 2

Last Fixed: 01/11/2018 at 04:43:59 AM (GMT-0800)

First Reopened: N/A

Last Reopened: N/A

Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

For more information, Customers are advised to refer the Security Update Guide. (https://portal.msrc.microsoft.com/en-us/security-guidance)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Microsoft Security Update Guide (https://portal.msrc.microsoft.com/en-us/security-guidance)

RESULTS:

%programfiles%\Internet Explorer\iexplore.exe found
%programfiles(x86)%\Internet Explorer\iexplore.exe found
KB4056892 is not installed
%windir%\System32\mshtml.dll Version is 11.0.16299.125
HKLM\Software\Microsoft\Internet Explorer Version = 9.11.16299.0

4 Microsoft Edge Security Update for January 2018 (ADV180002) (Spectre/Meltdown) CVSS: - CVSS3: 4.9 Fixed

| | | | |
|---|---|---|---|
| QID: | 91425 | CVSS Base: | 7.6 |
| Category: | Windows | CVSS Temporal: | 5.6 |
| CVE ID: | CVE-2018-0776, CVE-2018-0777, CVE-2018-0778, CVE-2018-0780, CVE-2018-0781, CVE-2018-0800, CVE-2018-0803, CVE-2018-0758, CVE-2018-0762, CVE-2018-0766, CVE-2018-0767, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0775, CVE-2017-5753, CVE-2017-5754, CVE-2017-5715 | | |
| Vendor Reference: | KB4056892, KB4056888, KB4056890, KB4056893, KB4056891, ADV180002 | | |
| Bugtraq ID: | 102371, 102376, 102378, 102405, 102408, 102388, 102393, 102395, 102396, 102397, 102409, 102398, 102399, 102400, 102401, 102402, 102403, 102389, 102404, 102392, 102384 | | |

| | | | |
|---|---|---|---|
| Service Modified: | 01/09/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.9 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Closed/Fixed | | |

First Detected: 01/05/2018 at 09:07:38 AM (GMT-0800)

Last Detected: 01/09/2018 at 01:02:56 PM (GMT-0800)

Times Detected: 3

Last Fixed: 01/11/2018 at 04:43:59 AM (GMT-0800)

First Reopened: N/A

Last Reopened: N/A

Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

For more information, customers are advised to refer the Security Update Guide. (https://portal.msrc.microsoft.com/en-us/security-guidance)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Microsoft Security Update Guide (https://portal.msrc.microsoft.com/en-us/security-guidance)

RESULTS:

KB4056892 is not installed
%windir%\System32\edgehtml.dll Version is 11.0.16299.125

## Information Gathered (1)

1 Processor Information for Windows Target System

| | |
|---|---|
| QID: | 43113 |
| Category: | Hardware |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 01/03/2018 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: 04/10/2017 at 11:02:27 AM (GMT-0700)

Last Detected: 01/15/2018 at 10:57:44 AM (GMT-0800)

Times Detected: 180

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:
n/a

RESULTS:
HKLM\System\CurrentControlSet\Control\Session Manager\Environment

| | | |
|---|---|---|
| PROCESSOR_IDENTIFIER | = | Intel64 Family 6 Model 61 Stepping 4, GenuineIntel |

## 192.168.254.215 (macbook-air-de-cyrille.local, MACBOOKAIR-1B08) Mac OS X 10.13.2
## Global Default Network

| Host Identification Information | |
|---|---|
| IPs | |
| Asset Id | cb54cb92-3414-4dd7-a6ed-e233755cbc9e |

| Vulnerabilities Total | 2 (+1) | Security Risk | 4.0 |
|---|---|---|---|

**by Status**

| Status | Confirmed | Potential | Total |
|---|---|---|---|
| New | 0 | - | 0 |
| Active | 1 | - | 1 |
| Re-Opened | 0 | - | 0 |
| Total | 1 | - | 1 |
| Fixed | 1 | - | 1 |
| Changed | 1 | - | 1 |

**by Severity**

| Severity | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| 5 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 4 | 1 | (+1) | - | | 0 | 1 | (+1) |
| 3 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 2 | 0 | (0) - | - | | 0 | 0 | (0) - |
| 1 | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 1 | (+1) | - | | 1 | 2 | (+1) |

**5 Biggest Categories**

| Category | Confirmed | (Trend) | Potential | (Trend) | Information Gathered | Total | (Trend) |
|---|---|---|---|---|---|---|---|
| Local | 1 | (+1) | - | | 0 | 1 | (+1) |
| Hardware | 0 | (0) - | - | | 1 | 1 | (0) - |
| Total | 1 | (+1) | - | | 1 | 2 | (+1) |

## Vulnerabilities (2)

4 Apple macOS High Sierra Supplemental Update / Safari 11.0.2 update (Spectre) CVSS: - CVSS3: 5.1 Active

| | | | |
|---|---|---|---|
| QID: | 370716 | CVSS Base: | 4.7 |
| Category: | Local | CVSS Temporal: | 3.7 |
| CVE ID: | CVE-2017-5753, CVE-2017-5715 | | |
| Vendor Reference: | HT208397, HT208403 | | |
| Bugtraq ID: | 102376, 102371 | | |
| Service Modified: | 01/09/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 5.1 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Open | | |

First Detected: 01/11/2018 at 05:30:44 AM (GMT-0800)
Last Detected: 01/17/2018 at 06:49:20 AM (GMT-0800)
Times Detected: 7
Last Fixed: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

The update can be downloaded and installed via Apple Downloads (http://support.apple.com/downloads/).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
HT208397: OS X High Sierra (https://support.apple.com/en-us/HT208397)
HT208403: Safari for Mac OS X (https://support.apple.com/en-us/HT208403)

RESULTS:

<key>CFBundleVersion</key>
<string>13604.4.7.1.3</string>

### 4 Mozilla Firefox Spectre Vulnerability (mfsa2018-01)(Spectre)

CVSS: - CVSS3: 4.9 Fixed

| | | | |
|---|---|---|---|
| QID: | 370712 | CVSS Base: | 4.7 |
| Category: | Local | CVSS Temporal: | 3.5 |
| CVE ID: | CVE-2017-5753, CVE-2017-5715 | | |
| Vendor Reference: | mfsa2018-01 | | |
| Bugtraq ID: | 102371, 102376 | | |
| Service Modified: | 01/05/2018 | CVSS3 Base: | 5.6 |
| User Modified: | - | CVSS3 Temporal: | 4.9 |
| Edited: | No | | |
| PCI Vuln: | Yes | | |
| Ticket State: | Closed/Fixed | | |

First Detected: 01/06/2018 at 04:48:24 PM (GMT-0800)

Last Detected: 01/15/2018 at 04:17:57 AM (GMT-0800)

Times Detected: 10

Last Fixed: 01/15/2018 at 05:10:27 PM (GMT-0800)

First Reopened: N/A

Last Reopened: N/A

Times Reopened: N/A

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

The vendor has issued a fix (57.0.4).
Refer to MFSA 2018-01 (https://www.mozilla.org/en-US/security/advisories/)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
MFSA 2018-01: MAC OS X (https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/)
MFSA 2018-01: Windows (https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/)

RESULTS:

Found Vulnerable Firefox Version prior to 57.0.4

## Information Gathered (1)

1 Apple Macintosh Processor Architecture

| | |
|---|---|
| QID: | 43110 |
| Category: | Hardware |
| CVE ID: | - |
| Vendor Reference: | - |
| Bugtraq ID: | - |
| Service Modified: | 01/03/2018 |
| User Modified: | - |
| Edited: | No |
| PCI Vuln: | No |
| Ticket State: | |

First Detected: N/A

Last Detected: 01/17/2018 at 06:49:20 AM (GMT-0800)

Times Detected: 358

CVSS Environment:

| | |
|---|---|
| Asset Group: | - |
| Collateral Damage Potential: | - |
| Target Distribution: | - |
| Confidentiality Requirement: | - |
| Integrity Requirement: | - |
| Availability Requirement: | - |

SOLUTION:

N/A

RESULTS:

Processor Name: Intel Core i5
Processor Speed: 1,7 GHz
Number of Processors: 1
Total Number of Cores: 2
L2 Cache (per Core): 256 KB

## Footnotes

This footnote indicates that the CVSS Base score that is displayed for the vulnerability is not supplied by NIST. When the service looked up the latest NIST score for the vulnerability, as published in the National Vulnerability Database (NVD), NIST either listed the CVSS Base score as 0 or did not provide a score in the NVD. In this case, the service determined that the severity of the vulnerability warranted a higher CVSS Base score. The score provided by the service is displayed.



Customized Spectre/Meltdown Reporting Tracking Template as per https://community.qualys.com/docs/DOC-6331