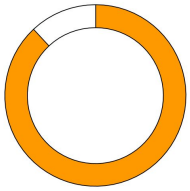
Intel Security Vulnerabilities 2019.2
November 2019

Category: Various

Highest CVSSv3 Score: 8.8



Advisory ID	nutanix-sa-017-2019
Last Updated	13 May 2020
Published	12 November 2019
Version	7

CVE(s)

CVE-2019-11109
CVE-2019-0185
CVE-2019-0139
CVE-2019-0140
CVE-2019-0143
CVE-2019-0144
CVE-2019-0145
CVE-2019-0146
CVE-2019-0147
CVE-2019-0148
CVE-2019-0149
CVE-2019-0150
CVE-2019-11135
CVE-2019-11139
CVE-2018-12207

Final Update

Summary

Intel, as part of their Platform Update for 2019.2, has released 13 security advisories, 4 functional updates and 5 additional advisories were part of their regular monthly update process. Not all of the above 18 advisories apply to the Nutanix software or platforms. This Security Advisory will only list those that apply to Nutanix products, and the applicable CVE IDs.

Information on Vulnerabilities

CVE-2019-11109

Logic issue in subsystem in Intel(R) Server Platform Services before versions SPS_E5_04.01.04.297.0, SPS_SoC-X_04.00.04.101.0, SPS_SoC-A_04.00.04.193.0 may allow a privileged user to potentially enable Denial of Service via local access.

CVSS Base Score: 4.4 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

Reference: INTEL-SA-00241 [intel.com]

CVE-2019-0185

Insufficient access control in protected memory subsystem for Intel(R) System Management Mode for 6th, 7th, 8th , 9th and 10th Generation Intel(R) Core(TM) Processor Families, Intel(R) Xeon(R) Processor E3-1500 v5 and v6 Families, Intel(R) Xeon(R) E-2100 and E-2200 Processor Families with Intel(R) Processor Graphics may allow a privileged user to potentially enable information disclosure of System Management Memory via local access.

CVSS Base Score: 6.0 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N

Reference: INTEL-SA-00254 [intel.com]

CVE-2019-0139

Insufficient access control in firmware for Intel(R) Ethernet 700 Series Controllers before version 7.0 may allow a privileged user to potentially enable an escalation of privilege, denial of service, or information disclosure via local access.

CVSS Base Score: 6.7 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Reference: INTEL-SA-00255 [intel.com]

CVE-2019-0140

Buffer overflow in firmware for Intel(R) Ethernet 700 Series Controllers before version 7.0 may allow an unauthenticated user to potentially enable an escalation of privilege via an adjacent access.

CVSS Base Score: 8.8 High

CVSS Vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Reference: INTEL-SA-00255 [intel.com]

CVE-2019-0143

Unhandled exception in Kernel-mode drivers for Intel(R) Ethernet 700 Series Controllers versions before 17MAY2019 may allow an authenticated user to potentially enable a denial of service via local access.

CVSS Base Score: 4.4 Medium

Tel: 1 (855) 688-2649 | Fax: 1 (408) 916-4039 | Email: info@nutanix.com

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L

Reference: INTEL-SA-00255 [intel.com]

CVE-2019-0144

Unhandled exception in firmware for Intel(R) Ethernet 700 Series Controllers before version 7.0 may allow an authenticated user to potentially enable a denial of service via local access.

CVSS Base Score: 6.5 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

Reference: INTEL-SA-00255 [intel.com]

CVE-2019-0145

Buffer overflow in i40e driver for Intel(R) Ethernet 700 Series Controllers versions before 2.8.43 may allow an authenticated user to potentially enable an escalation of privilege via local access.

CVSS Base Score: 7.8 High

CVSS Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Reference: INTEL-SA-00255 [intel.com]

CVE-2019-0146

Resource leak in i40e driver for Intel(R) Ethernet 700 Series Controllers versions before 2.8.43 may allow an authenticated user to potentially enable a denial of service via local access.

CVSS Base Score: 6.5 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

Reference: INTEL-SA-00255 [intel.com]

CVE-2019-0147

Insufficient input validation in i40e driver for Intel(R) Ethernet 700 Series Controllers versions before 2.8.43 may allow an authenticated user to potentially enable a denial of service via local access.

CVSS Base Score: 5.6 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:N/A:H

Tel: 1 (855) 688-2649 | Fax: 1 (408) 916-4039 | Email: info@nutanix.com

Reference: INTEL-SA-00255 [intel.com]

CVE-2019-0148

Resource leak in i40e driver for Intel(R) Ethernet 700 Series Controllers versions before 2.8.43 may allow an authenticated user to potentially enable a denial of service via local access.

CVSS Base Score: 6.5 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

Reference: INTEL-SA-00255 [intel.com]

CVE-2019-0149

Insufficient input validation in i40e driver for Intel(R) Ethernet 700 Series Controllers versions before 2.8.43 may allow an authenticated user to potentially enable a denial of service via local access.

CVSS Base Score: 6.5 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

Reference: INTEL-SA-00255 [intel.com]

CVE-2019-0150

Insufficient access control in firmware Intel(R) Ethernet 700 Series

Controller versions before 7.0 may allow a privileged user to potentially enable a denial of service via local access.

CVSS Base Score: 6.0 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H

Reference: INTEL-SA-00255 [intel.com]

CVE-2019-11135

TSX Asynchronous Abort (TAA) condition on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

CVSS Base Score: 6.5 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

Reference: INTEL-SA-00270 [intel.com]

CVE-2019-11139

A vulnerability in voltage modulation for some Intel(R) Xeon(R) Scalable Processors CPUs may allow a privileged user to potentially enable denial of service via local access.

CVSS Base Score: 5.8 Medium

CVSS Vector: CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:L/A:H

Reference: INTEL-SA-00271 [intel.com]

CVE-2018-12207

Improper page table invalidation for page table updates by a virtual guest operating system for multiple Intel(R) platforms may allow an authenticated user to potentially enable temporary denial of service of the host system via local access.

CVSS Base Score: 6.5 Medium

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:T/RC:C/CR:H/AR:M

Reference: INTEL-SA-00210 [intel.com]

Affected Products

This document will be updated with the patch release schedules. Please check the Nutanix Support Portal for the latest update.

Nutanix Products

Product	Fix Release
AHV (Ethernet 700 Series) Applicable CVEs: CVE-2019-0139, CVE-2019-1040, CVE-2019-0143, CVE-2019-0145, CVE-2019-0146, CVE-2019-0147, CVE-2019-0148, CVE-2019-0149, CVE-2019-0150 Severity Ranges: 4.4 - 8.8	*Now available via AOS 5.11.2, 5.10.8 and 5.16 or higher, and as part of AHV version 20170830.337 or higher on the Nutanix Support Portal.*
AHV (MCU, Page Tables) Applicable CVEs: CVE-2018-12207, CVE-2019-11135, CVE-2019-11139 Severity Ranges: 5.8 - 6.5	*Now available via AOS 5.16 and 5.11.3 as part of AHV version 20190916.81 on the Nutanix Support Portal.*
Foundation (Ethernet 700 Series) Applicable CVEs: CVE-2019-0139, CVE-2019-0140, CVE-2019-0143, CVE-2019-0144, CVE-2019-0145, CVE-2019-0146, CVE-2019-0147, CVE-2019-0148, CVE-2019-0149, CVE-2019-0150 Severity Ranges: 4.4 - 8.8	*Now available via Foundation 4.5 and newer on the Nutanix Support Portal.* *NOTE: CVEs cover both a driver and firmware component. Foundation is affected because it can deliver hardware drivers for specific versions of ESXi and Hyper-V on NX hardware.* *NX hardware with x710 series controllers already ship with Firmware 7.0.*
NX Platforms (G6 and G7) Applicable CVEs: CVE-2019-11109, CVE-2019-0185, CVE-2019-11135, CVE-2019-11139, CVE-2018-12207 Severity Ranges: 4.4 - 6.0	*Now available via LCM 2.3.1 on the Nutanix Support Portal.*

3rd Party Products

Product	Fix Release
Lenovo	*Driver and firmware updates for Dell and Lenovo hardware utilizing a x710 series adapter will be provided by the OEM. Once available, links to the advisories will be provided here.*
Dell	

Sources

Intel Product Security Center
(https://www.intel.com/content/www/us/en/security-center/default.html)
INTEL-SA-00241
((https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00241.html)
INTEL-SA-00254
(https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00254.html)
INTEL-SA-00255
(https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00255.html)
INTEL-SA-00270
(https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00270.html)
INTEL-SA-00271
(https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00271.html)
INTEL-SA-00210
(https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00210.html)

Support

If you have questions, please open a case with Nutanix Support at http://portal.nutanix.com, or by calling Support at the phone number on the website http://www.nutanix.com/support.

Thank you for being a Nutanix customer.

Revision History

Version	Section	Date
1	-	12 November 2019
2	Minor updates	20 November 2019
3	Release Timeline Updates	05 December 2019
4	Release Timeline Updates	18 December 2019
5	Releases updated	16 January 2020
6	Verification of timelines	12 February 2020
7	Final update	13 May 2020

Tel: 1 (855) 688-2649 | Fax: 1 (408) 916-4039 | Email: info@nutanix.com