Advisory Alert

Alert Number: **AAA20230216** **Date:** **February 16, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Heap-based buffer overflow Vulnerability
Cisco	**High** , **Medium**	Multiple Vulnerabilities
Splunk	**High** , **Medium**	Multiple Vulnerabilities
HP	**High** , **Medium**, **Low**	Multiple Vulnerabilities
IBM	**Low**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Heap-based buffer overflow Vulnerability (CVE-2023-20032)
Description	Cisco has released a Security Update addressing buffer overflow Vulnerability that exist in their products. A Vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition Cisco highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Secure Web Appliance - before 15.0.0-254 Secure Endpoint Private Cloud - before 3.6.0 Secure Endpoint for Windows - before 8.1.5 Secure Endpoint for macOS - before 1.21.1 Secure Endpoint for Linux - before 1.20.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy

Affected Product	**Cisco**
Severity	**High** , **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20014, CVE-2023-20009, CVE-2023-20075, CVE-2023-20052, CVE-2022-20952, CVE-2023-20053, CVE-2023-20085)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could cause Denial of Service, Input validation error, OS Command Injection, File Parsing XML Entity Expansion, Content Encoding Filter Bypass, Cross-Site Scripting. Cisco recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Cisco AsyncOS for Web Security Appliances - 14.0.1-053 Cisco Email Security Appliance - before 14.3.0-032 Cisco Identity Services Engine (ISE) - before 3.2 P1 Cisco Secure Email and Web Manager - before 14.3.0-120 Nexus Dashboard - before 2.3(1c) Secure Endpoint for Linux - before 1.20.2 Secure Endpoint for macOS - before 1.21.1 Secure Endpoint for Windows - before 8.1.5 Secure Endpoint Private Cloud - before 3.6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndb-dnsdos-bYscZOsu https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-xxe-TcSZduhN https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-bwBfugek https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nexus-dashboard-xss-xc5BcgsQ https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-ubfHG75C

Affected Product	**Splunk**
Severity	**High , Medium**
Affected Vulnerability	Multiple Vulnerability (CVE-2023-22931, CVE-2023-22932, CVE-2023-22933, CVE-2023-22934, CVE-2023-22935, CVE-2023-22936, CVE-2023-22937, CVE-2023-22938, CVE-2023-22939, CVE-2023-22940, CVE-2023-22941, CVE-2023-22942, CVE-2023-22943, CVE-2022-42889)
Description	Splunk has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities to cause cross-site scripting (XSS) and Server Side Request Forgery, SPL Command Safeguards Bypass, Permissions Validation Failure, Cross-Site Request Forgery and HTTP after Certificate Validation Failure. Splunk recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Splunk Add-on Builder 4.1 cloudconnectlib 4.1.1 and lower 4.1.2 Splunk Cloud Platform - Search 8.2.2202 and lower 8.2.2203 Splunk Cloud Platform - Splunk Web 9.0.2208 and lower 9.0.2209 Splunk Cloud Platform Splunk Web 9.0.2209 and lower 9.0.2209.3 Splunk Cloud Platform - Splunk Web 9.0.2209 and lower 9.0.2212 Splunk Cloud Platform - Splunk Web 9.2.2209 and lower 9.0.2212 Splunk Cloud Platform - Splunk Web 9.2.2209 and lower 9.2.2209.3 Splunk CloudConnect SDK 3.1 - 3.1.2 and lower 3.1.3 Splunk Enterprise 8.1 Search 8.1.12 and lower 8.1.13 Splunk Enterprise 8.1 Splunk Web 8.1.12 and lower 8.1.13 Splunk Enterprise 8.2 Search 8.2.0 to 8.2.9 8.2.10 Splunk Enterprise 8.2 Splunk Web 8.2.0 to 8.2.9 8.2.10 Splunk Enterprise 9.0 Splunk Web 9.0. to 9.0.3 9.0.4 Splunk Enterprise 9.0 Splunk Web 9.0.0 to 9.0.3 9.0.2209.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://advisory.splunk.com/?301=/en_us/product-security.html#quarterly-security-patch-updates

Affected Product	**HP**
Severity	**High, Medium , Low**
Affected Vulnerability	Multiple Vulnerability (CVE-2021-0187, CVE-2022-26343, CVE-2022-26837, CVE-2022-32231, CVE-2022-21216, CVE-2022-36348, CVE-2022-33972, CVE-2022-38090, CVE-2022-33196, CVE-2021-0187, CVE-2022-21216, CVE-2022-36794, CVE-2022-30704)
Description	HP has released Security Updates addressing multiple vulnerabilities that exist in their Intel processors. Security vulnerabilities in HP servers using certain Intel processors could be locally exploited to allow escalation of privilege, disclosure of information. HP recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	HPE ProLiant BL460c Gen10 Server Blade - Prior to 2.76_02-09-2023 HPE ProLiant DL110 Gen10 Plus Telco server -prior to 1.72_02-02-2023 HPE ProLiant DL110 Gen10 Plus Telco server -Prior to SPS_E5_04.04.04.300.0 HPE ProLiant DL160 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant DL180 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant DL20 Gen10 Plus server -prior to 1.68_01-12-2023 HPE ProLiant DL20 Gen10 Plus server -Prior to SPS_E3_06.00.03.300.0 HPE ProLiant DL20 Gen10 Server -prior to 2.68_01-12-2023 HPE ProLiant DL360 Gen10 Plus server -prior to 1.72_02-02-2023 HPE ProLiant DL360 Gen10 Plus server -Prior to SPS_E5_04.04.04.300.0 HPE ProLiant DL360 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant DL380 Gen10 Plus server -prior to 1.72_02-02-2023 HPE ProLiant DL380 Gen10 Plus server -Prior to SPS_E5_04.04.04.300.0 HPE ProLiant DL380 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant DL560 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant DX360 Gen10 Plus server - Prior to 1.72_02-02-2023 HPE ProLiant DX360 Gen10 Plus server - Prior to SPS 04.04.04.300 HPE ProLiant DX360 Gen10 server - Prior to 2.76_02-09-2023 HPE ProLiant DX380 Gen10 Plus server - Prior to 1.72_02-02-2023 HPE ProLiant DX380 Gen10 Plus server - Prior to SPS 04.04.04.300 HPE ProLiant DX380 Gen10 server - Prior to 2.76_02-09-2023 HPE ProLiant DX560 Gen10 server - Prior to 2.76_02-09-2023 HPE ProLiant MicroServer Gen10 Plus v2 -prior to 1.68_01-12-2023 HPE ProLiant MicroServer Gen10 Plus v2 -Prior to SPS_E3_06.00.03.300.0 HPE ProLiant ML110 Gen10 Server -prior to 2.76_02-09-2023 HPE ProLiant ML30 Gen10 Plus server -prior to 1.68_01-12-2023 HPE ProLiant ML30 Gen10 Plus server -Prior to SPS_E3_06.00.03.300.0 HPE ProLiant ML30 Gen10 Server -prior to 2.68_01-12-2023 HPE ProLiant ML350 Gen10 Server -prior to 2.76_02-09-2023 HPE Storage File Controller - Prior to 2.76_02-09-2023 HPE Storage Performance File Controller - Prior to 2.76_02-09-2023 HPE StoreEasy 1460 Storage - Prior to 2.76_02-09-2023 HPE StoreEasy 1560 Storage - Prior to 2.76_02-09-2023 HPE StoreEasy 1660 Expanded Storage - Prior to 2.76_02-09-2023 HPE StoreEasy 1660 Performance Storage - Prior to 2.76_02-09-2023 HPE StoreEasy 1660 Storage - Prior to 1.72_02-02-2023 (U46 ROM Family) HPE StoreEasy 1660 Storage - Prior to 2.76_01-18-2023 (U30 ROM Family) HPE StoreEasy 1660 Storage - Prior to SPS_E5_04.04.04.300.0 (U46 ROM Family) HPE StoreEasy 1860 Performance Storage - Prior to 2.76_02-09-2023 HPE StoreEasy 1860 Storage - Prior to 1.72_02-02-2023 (U46 ROM Family) HPE StoreEasy 1860 Storage - Prior to 2.76_01-18-2023 (U30 ROM Family) HPE StoreEasy 1860 Storage - Prior to SPS_E5_04.04.04.300.0 (U46 ROM Family) HPE Superdome Flex 280 Server -Prior to 1.40.60 HPE Synergy 480 Gen10 Compute Module - Prior to 2.76_02-09-2023 HPE Synergy 480 Gen10 Plus Compute Module - Prior to 1.72_02-02-2023 HPE Synergy 480 Gen10 Plus Compute Module - Prior to SPS 04.04.04.300 HPE Synergy 660 Gen10 Compute Module - Prior to 2.76_02-09-2023
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/connect/s/securitybulletinlibrary?language=en_US

Affected Product	**IBM**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-43929, CVE-2022-43927, CVE-2014-3577, CVE-2022-43930, CVE-2022-31129, CVE-2022-45787)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of the most severe vulnerabilities could lead to information discloser, denial of service. IBM recommends to apply the necessary security updates at your earliest to avoid issues
Affected Products	IBM WebSphere Remote Server 9.0, 8.5 QRadar Advisor 2.5 - 2.6.3 IBM WebSphere Application Server Liberty: 21.0.0.12 - 23.0.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6955861 https://www.ibm.com/support/pages/node/6955819 https://www.ibm.com/support/pages/node/6953779

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.