Advisory Alert

Alert Number: AAA20230302 **Date:** March 2, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Dell	**High**	Version Disclosure Vulnerability
Lenovo	**High**	Multiple Vulnerabilities
HP	**High, Medium**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-20078, CVE-2023-20079)
Description	Cisco has released a Security Update addressing Multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause Command Injection and Denial of Service. **CVE-2023-20078**- A Command Injection vulnerability exists due to improper input validation in the web-based management interface. A remote unauthenticated attacker can pass specially crafted data to the application and execute arbitrary OS commands on the target system. **CVE-2023-20079**- A denial of service vulnerability exists due to insufficient validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	IP Phone 6800 Series with Multiplatform Firmware IP Phone 7800 Series with Multiplatform Firmware IP Phone 8800 Series with Multiplatform Firmware Unified IP Conference Phone 8831 Unified IP Conference Phone 8831 with Multiplatform Firmware Unified IP Phone 7900 Series
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Version Disclosure Vulnerability (CVE-2023-25544, CVE-2023-24567)
Description	Dell has released a Security Update addressing Version Disclosure Vulnerability that exist in their products. Attackers can exploit these vulnerabilities to launch target-specific attacks. **CVE-2023-25544**- An Apache Tomcat version disclosure vulnerability exists in Dell Networker versions 19.5 and earlier. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and launch target-specific attacks. **CVE-2023-24567**- RabbitMQ version disclosure vulnerability exists in Dell Networker versions 19.5 and earlier. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and launch target-specific attacks. Dell recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Dell NetWorker, 19.5 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000210471/dsa-2023-058-dell-networker-security-update-for-version-disclosure-vulnerability

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1017, CVE-2023-1018)
Description	Lenovo has released a Security Update addressing multiple Vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause Information Disclosure, Escalation of Privilege. **CVE-2023-1017**- An out-of-bounds write vulnerability exists in TPM2.0's Module Library allowing writing of a 2-byte data past the end of TPM2.0 command in the CryptParameterDecryption routine. Successful exploitation can lead to denial of service (crashing the TPM chip/process or rendering it unusable) and/or arbitrary code execution in the TPM context. **CVE-2023-1018**- RabbitMQ version disclosure vulnerability exists in Dell Networker versions 19.5 and earlier. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and launch target-specific attacks. Lenovo recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	NPCT65x TPM in 2.0 mode (only) with firmware 1.3.0.1, 1.3.1.0 & 1.3.2.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/lk/en/product_security/LEN-118374 https://support.lenovo.com/lk/en/product_security/LEN-118320

Affected Product	**HP**
Severity	**High** , **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-33196, CVE-2022-33972)
Description	HP has released Security Updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause privilege escalation and information disclosure. **CVE-2023-33196**- A privilege escalation vulnerability exists due to incorrect default permissions for memory controller configurations for some Intel Xeon processors when using Intel Software Guard Extensions. Using this vulnerability a local user can escalate privileges on the system. **CVE-2023-33972**- An information disclosure vulnerability in HPE Edgeline servers that use certain Intel processors that allows a local privileged user to enable information disclosure. HP recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	HPE Edgeline e920 Server Blade - Prior to 1.66_02-02-2023 HPE Edgeline e920d Server Blade - Prior to 1.66_02-02-2023 HPE Edgeline e920t Server Blade - Prior to 1.66_02-02-2023
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04407en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04411en_us

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20104, CVE-2023-20088, CVE-2023-20061, CVE-2023-20062, CVE-2023-20069)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause Cross-Site Scripting, Denial of Service and server-side request forgery. Cisco recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Cisco Webex App for Web Cisco Finesse Release 12.6(2) and earlier Cisco Unified Intelligence Center Release 12.5 and earlier Cisco Unified Intelligence Center 12.6 Packaged Contact Center Enterprise (PCCE) Unified Contact Center Enterprise (UCCE) Unified Contact Center Express (UCCX) Cisco Prime Infrastructure Earlier than 3.10.3 Cisco EPN Manager Earlier than 7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-proxy-dos-vY5dQhrV https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-Yn8HHsMJ https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-infodisc-ssrf-84ZBmwVk https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pi-epnm-xss-mZShH2J

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.