TLP: WHITE

Advisory Alert

Alert Number: AAA20230908 **Date:** September 8, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Authentication Bypass Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
HPE	**High**, Medium	Multiple Vulnerabilities
Qnap	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2023-20238)
Description	Cisco has released a security update addressing an Authentication Bypass Vulnerability that exist in their products. **CVE-2023-20238** - A vulnerability in the single sign-on (SSO) implementation of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks Xtended Services Platform could allow an unauthenticated, remote attacker to forge the credentials required to access an affected system. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Products running a vulnerable release of Cisco BroadWorks and have one of the following applications enabled: • AuthenticationService • BWCallCenter • BWReceptionist • CustomMediaFilesRetrieval • ModeratorClientApp • PublicECLQuery • PublicReporting • UCAPI • Xsi-Actions • Xsi-Events • Xsi-MMTel • Xsi-VTR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-auth-bypass-kCggMWhX

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2017-9765, CVE-2019-7659, CVE-2020-13576)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in third party products that in turn affect Dell products. **CVE-2017-9765 -** Integer overflow in the soap_get function in Genivia gSOAP 2.7.x and 2.8.x before 2.8.48, as used on Axis cameras and other devices, allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer overflow and application crash) via a large XML document **CVE-2019-7659** - Genivia gSOAP 2.7.x and 2.8.x before 2.8.75 allows attackers to cause a denial of service (application abort) or possibly have unspecified other impact if a server application is built with the -DWITH_COOKIES flag. This affects the C/C++ libgsoapck/libgsoapck++ and libgsoapssl/libgsoapssl++ libraries, as these are built with that flag. **CVE-2020-13576** - A code execution vulnerability exists in the WS-Addressing plugin functionality of Genivia gSOAP 2.8.107. A specially crafted SOAP request can lead to remote code execution. An attacker can send an HTTP request to trigger this vulnerability. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell NetWorker vProxy • Version 19.7.1 • Versions 19.7 through 19.7.0.5 • Versions 19.8 through 19.8.0.2 • Versions 19.9 through 19.9.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000217446/dsa-2023-267-security-update-for-dell-networker-vproxy-gsoap-vulnerabilities

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20243, CVE-2023-20250, CVE-2023-20193, CVE-2023-20194, CVE-2023-20263)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Out-of-bounds write, Use-after-free condition, Stack-out-of-bounds-read, Unauthorized command execution. Cisco recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Cisco Hyperflex HX Data Platform Versions Earlier than 5.0, 5.0 and 5.5 Cisco ISE PSNs that are configured with RADIUS Cisco ISE Release 2.7 and earlier, 3.0, 3.1, 3.2, and 3.3 Cisco RV110W Wireless-N VPN Firewalls Cisco RV130 VPN Routers Cisco RV130W Wireless-N Multifunction VPN Routers Cisco RV215W Wireless-N VPN Router
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-radius-dos-W7cNn7gt https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-stack-SHYv2f5N https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-priv-esc-KJLp2Aw https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-redirect-UxLgqdUF

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38484, CVE-2023-38485, CVE-2023-38486, CVE-2023-30908, CVE-2022-4304, CVE-2023-2650)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Authentication Bypass, Denial of Service (DoS), Disclosure of Sensitive Information, Compromise of System Integrity and Execution of Arbitrary Code With Root Privileges. HPE recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	ArubaOS 10.4.x.x: 10.4.0.1 and below ArubaOS 8.11.x.x: 8.11.1.0 and below ArubaOS 8.10.x.x: 8.10.0.6 and below ArubaOS 8.6.x.x: 8.6.0.21 and below Hewlett Packard Enterprise OneView v8.5 or later Hewlett Packard Enterprise OneView v6.60.05 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04535en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04530en_us

Affected Product	**Qnap**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2023-23357, CVE-2023-23356, CVE-2023-23354, CVE-2022-27599)
Description	Qnap has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Cross-site scripting (XSS), Command injection, and Sensitive information disclosure. Qnap recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	QuLog Center 1.5, 1.4, 1.3 QuFirewall 2.3 QVR Pro Client 2.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-23-16 https://www.qnap.com/en/security-advisory/qsa-23-14 https://www.qnap.com/go/security-advisory/qsa-23-13 https://www.qnap.com/go/security-advisory/qsa-23-08

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.