Advisory Alert

Alert Number: AAA20241107 **Date:** November 7, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Improper Input Validation Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Multiple Vulnerabilities
HPE	**High**	OpenSSH RegreSSHion Vulnerability
Veeam	**High**	Authentication Bypass Vulnerability
F5	**High**, Medium	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Drupal	**High**, Medium	Multiple Vulnerabilities
NetGear	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Improper Input Validation Vulnerability (CVE-2024-20418)
Description	Cisco has released security updates addressing an Improper Input Validation Vulnerability that exists in Cisco Unified Industrial Wireless Software. **CVE-2024-20418** - Due to an improper validation of input to the web-based management interface, an attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system of the affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following Cisco products if they are running on Cisco Unified Industrial Wireless Software Release 17.15, 17.14 & earlier and have the URWB operating mode enabled: • Catalyst IW9165D Heavy Duty Access Points • Catalyst IW9165E Rugged Access Points and Wireless Clients • Catalyst IW9167E Heavy Duty Access Points
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-backhaul-ap-cmdinj-R7E28Ecs

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Dell EMC VxRail Appliance Versions prior to 8.0.310 • Dell Secure Connect Gateway Version 5.24.00.14 • Dell Avamar Server Hardware Appliance Gen4T/ Gen5A Versions 19.4, 19.7, 19.8, 19.9, 19.10, 19.10-SP1 running SUSE Linux Enterprise 12 SP5 • Dell Avamar Virtual Edition Versions 19.4, 19.7, 19.8, 19.9, 19.10, 19.10-SP1 running SUSE Linux Enterprise 12 SP5 (including Azure and AWS deployments) • Dell Avamar NDMP Accelerator Versions 19.4, 19.7, 19.8, 19.9, 19.10, 19.10-SP1 running SUSE Linux Enterprise 12 SP5 • Dell Avamar VMware Image Proxy Versions 19.4, 19.7, 19.8, 19.9, 19.10, 19.10-SP1 running SUSE Linux Enterprise 12 SP5 • Dell Networker Virtual Edition (NVE) Versions 19.4.x, 19.5.x, 19.6.x, 19.7.x, 19.8.x, 19.9.x, 19.10.x, 19.11.x running SUSE Linux Enterprise 12 SP5 • Dell Power Protect DP Series Appliance / Dell Integrated Data Protection Appliance (IDPA) Version 2.7.x running on SLES12SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000240575/dsa-2024-393-security-update-for-dell-vxrail-hci-8-0-310-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000237211/dsa-2024-407-dell-secure-connect-gateway-security-update-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000245131/dsa-2024-433-security-update-for-dell-avamar-dell-networker-virtual-edition-nve-and-dell-powerprotect-dp-series-appliance-dell-integrated-data-protection-appliance-idpa-security-update-for-multiple-vulnerabilities

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-37903, CVE-2023-37466, CVE-2024-45590, CVE-2024-43796, CVE-2024-43799, CVE-2024-45296, CVE-2024-43800)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in Unified OSS Console Assurance Monitoring (UOCAM) Software. These vulnerabilities could be exploited by malicious users to cause Local/Remote Arbitrary Code Execution and Denial of Service conditions. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Unified OSS Console (UOC) versions prior to 3.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04727en_us&docLocale=en_US

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	OpenSSH RegreSSHion Vulnerability (CVE-2024-6387)
Description	HPE has released security updates addressing the OpenSSH RegreSSHion Vulnerability that exists in certain HPE Cray servers. **CVE-2024-6387** - A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Cray EX235a Accelerator Blade - CcNc firmware Prior to 1.9.5-39 HFP - 24.8.1 (8/28/2024) HPE Cray EX235n Server - CcNc firmware Prior to 1.9.5-39 HFP - 24.8.1 (8/28/2024) HPE Cray EX255a Accelerator Blade - CcNc firmware Prior to 1.9.5-39 HFP - 24.8.1 (8/28/2024) HPE Cray EX420 Compute Blade - CcNc firmware Prior to 1.9.5-39 HFP - 24.8.1 (8/28/2024) HPE Cray EX425 Compute Blade - CcNc firmware Prior to 1.9.5-39 HFP - 24.8.1 (8/28/2024) HPE Cray EX4252 Compute Blade - CcNc firmware Prior to 1.9.5-39 HFP - 24.8.1 (8/28/2024) HPE Cray EX254n Accelerator Blade - CcNc firmware Prior to 1.9.5-39 HFP - 24.8.1 (8/28/2024)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04733en_us&docLocale=en_US

Affected Product	**Veeam**
Severity	**High**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2024-40715)
Description	Veeam has released security updates addressing an Authentication Bypass Vulnerability that exists in Veeam Backup Enterprise Manager. **CVE-2024-40715** - This vulnerability in Veeam Backup Enterprise Manager allows attackers to bypass the authentication while performing a Man-in-the-Middle (MITM) attack. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication 10, 11, 12, 12.1, 12.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4682

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-3596, CVE-2022-38083, CVE-2024-10318)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-3596** - RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature. **CVE-2022-38083** - Improper initialization in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access. **CVE-2024-10318** - A session fixation issue was discovered in the NGINX OpenID Connect reference implementation, where a nonce was not checked at login time. This flaw allows an attacker to fix a victim's session to an attacker-controlled account. As a result, although the attacker cannot log in as the victim, they can force the session to associate it with the attacker-controlled account, leading to potential misuse of the victim's session. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (APM) 17.1.0 - 17.1.1 BIG-IP (all modules) 17.1.0 - 17.1.1, 16.1.0 - 16.1.4, 15.1.0 - 15.1.10 F5OS-A 1.7.0, 1.5.1 - 1.5.2 NGINX Instance Manager 2.5.0 - 2.17.3 NGINX API Connectivity Manager 1.3.0 - 1.9.2 NGINX Ingress Controller 3.0.0 - 3.7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000141008 • https://my.f5.com/manage/s/article/K000137202 • https://my.f5.com/manage/s/article/K000148232

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20371, CVE-2024-20540, CVE-2024-20507, CVE-2024-20511, CVE-2024-20514, CVE-2024-20504, CVE-2024-20457, CVE-2024-20537, CVE-2024-20538, CVE-2024-20539, CVE-2024-20525, CVE-2024-20527, CVE-2024-20528, CVE-2024-20476, CVE-2024-20487, CVE-2024-20533, CVE-2024-20534, CVE-2024-20445, CVE-2024-20484, CVE-2024-20536)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause SQL Injection, Denial of Service, Information Disclosure, Cross-Site Scripting, Authorization Bypass. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-3550-acl-bypass-mhskZc2q • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccmp-sxss-qBTDBZDD • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmm-info-disc-9ZEMAhGA • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-SVCkMMW • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnmpi-sxss-yyf2zkXs • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-xss-zYm3f49n • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-inf-disc-cUPKuA5n • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-auth-bypass-BBRf7mkE • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-vuln-DBQdWRy • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-vulns-AF544ED5 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mpp-xss-8tAV2TvF • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-infodisc-sbyqQVbG • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-dos-Oqb9uFEv • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-sqli-CyPPAxrL

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Access bypass and Cross site scripting. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basic HTTP Authentication module for Drupal 7.x prior to 7.x-1.4 Tooltip module prior to 1.1.2 of Drupal 8.x, 9.x or 10.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-058 • https://www.drupal.org/sa-contrib-2024-057

Affected Product	**NetGear**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	NetGear has released security updates addressing multiple vulnerabilities that exist in their Routers and Access Points. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Command Injection, Denial of Service and Security Misconfigurations. NetGear advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WAX630E firmware versions prior to 10.8.8.7 XR1000 firmware versions prior to 1.0.0.74 XR1000v2 firmware versions prior to 1.1.1.22
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://kb.netgear.com/000066408/Security-Advisory-for-Sensitive-Information-Disclosure-on-Some-Routers-PSV-2023-0117?article=000066408 • https://kb.netgear.com/000066407/Security-Advisory-for-Security-Misconfiguration-on-Some-Access-Points-PSV-2023-0141?article=000066407 • https://kb.netgear.com/000066409/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-Routers-PSV-2023-0109?article=000066409 • https://kb.netgear.com/000066410/Security-Advisory-for-Denial-of-Service-on-Some-Routers-PSV-2023-0047?article=000066410

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.