Advisory Alert

Alert Number: AAA20240906 **Date:** September 6, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Multiple Vulnerabilities
Juniper	**Critical**	Multiple Vulnerabilities
VMWare Broadcom	**Critical**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Dell	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Cisco	**Medium**	Sensitive Information Disclosure Vulnerability
OpenSSL	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-50782, CVE-2023-52425, CVE-2020-25659, CVE-2024-0450, CVE-2020-29651, CVE-2022-24805, CVE-2022-24806, CVE-2022-24807, CVE-2022-24808, CVE-2022-24809, CVE-2022-24810, CCVE-2024-20918, CVE-2024-20952, CVE-2024-20926, CVE-2023-4039, CVE-2021-3995, CVE-2021-3996, CVE-2020-14367)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products which affects Dell EMC Metronode. 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 Metronode versions prior to 8.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000228339/dsa-2024-380-security-update-for-dell-emc-metronode-for-multiple-third-party-components-vulnerabilities

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-41617, CVE-2021-28041, CVE-2021-31580, CVE-2016-20012, CVE-2021-36368, CVE-2023-25136, CVE-2023-48795, CVE-2023-51384, CVE-2023-51385, CVE-2023-38408)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in HP-UX Secure Shell. Exploitation of these vulnerabilities may lead to Information Disclosure, Arbitrary Command Execution, Authentication Bypass Compromise of System Integrity. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HP-UX 11i Secure Shell Software A.08.10.009 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbux04660en_us&docLocale=en_US

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in Juniper Secure Analytics. Exploitation of these vulnerabilities may lead to Information Disclosure, Arbitrary Code Execution, Directory Traversal, Denial of Service. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Juniper Secure Analytics versions prior to 7.5.0 UP9 IF02
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP9-IF02?language=en_US

Affected Product	**VMware Broadcom**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22954,CVE-2022-22955,CVE-2022-22956,CVE-2022-22957,CVE-2022-22958,CVE-2022-22959,CVE-2022-22960,CVE-2022-22961)
Description	Broadcom has released security updates addressing multiple vulnerabilities that exist in VMware products. Exploitation of these vulnerabilities may lead to Remote Code Execution, Authentication Bypass, Cross Site Request Forgery, Local Privilege Escalation, Information Disclosure. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Workspace ONE Access versions 21.08.0.1, 21.08.0.0 Running On Linux VMware Workspace ONE Access versions 20.10.0.1, 20.10.0.0 Running On Linux VMware Identity Manager (vIDM) versions 3.3.6, 3.3.5, 3.3.4, 3.3.3 Running On Linux VMware vRealize Automation version 7.6 Running On Linux VMware Cloud Foundation versions vIDM 4.x and vRA 3.x vRealize Suite Lifecycle Manager (vIDM) versions 8.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/23639

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-39338, CVE-2024-4068, CVE-2021-23727)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar Assistant. **CVE-2024-39338** - Axios is vulnerable to server-side request forgery, caused by a flaw with requests for path relative URLs get processed as protocol relative URLs. By sending a specially crafted request, an attacker could exploit this vulnerability to conduct SSRF attack. **CVE-2024-4068** - Node.js braces module is vulnerable to a denial of service, caused by the failure to limit the number of characters it can handle, leading to a memory exhaustion in lib/parse.js. By sending imbalanced braces as input, the parsing will enter a loop causing the JavaScript heap limit to be reached, and the program will crash. **CVE-2021-23727**- Celery could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted messages and metadata, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Assistant versions 1.0.0 - 3.7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7167607

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-39585, CVE-2024-38486, CVE-2024-42425, CVE-2024-42424)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their 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 Networking OS10 versions 10.5.6.x, 10.5.5.4 through 10.5.5.10 Precision 7920 Rack BIOS versions prior to 2.22.1 7920 XL Rack BIOS versions prior to 2.22.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000228357/dsa-2024-377-security-update-for-dell-networking-os10-vulnerability • https://www.dell.com/support/kbdoc/en-us/000228355/dsa-2024-376-security-update-for-dell-networking-os10-vulnerability • https://www.dell.com/support/kbdoc/en-us/000227015/dsa-2024-328 • https://www.dell.com/support/kbdoc/en-us/000227014/dsa-2024-327

Affected Product	**F5**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-17541, CVE-2021-31566, CVE-2021-23177, CVE-2018-1000877, CVE-2018-1000878, CVE-2022-36227, CVE-2024-21134)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Arbitrary Code Execution, Privilege Escalation, Information Disclosure. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Traffix SDC version 5.1.0, 5.2.0 BIG-IP (all modules) versions 17.1.0 - 17.1.1, 16.1.0 - 16.1.5, 15.1.0 - 15.1.10 BIG-IQ Centralized Management versions 8.2.0 - 8.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000140960 • https://my.f5.com/manage/s/article/K000140963 • https://my.f5.com/manage/s/article/K000140961 • https://my.f5.com/manage/s/article/K000140964 • https://my.f5.com/manage/s/article/K000140954 • https://my.f5.com/manage/s/article/K000140908

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Sensitive Information Disclosure Vulnerability (CVE-2024-20466)
Description	Cisco has released security updates addressing a Sensitive Information Disclosure Vulnerability that exists in Cisco Identity Services Engine. **CVE-2024-20466** - Due to an improper enforcement of administrative privilege levels for high-value sensitive data, an attacker with read-only Administrator privileges for the web-based management interface on an affected device could exploit the by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Identity Services Engine 2.7 and earlier, 3.0, 3.1, 3.2, 3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-exp-vdF8Jbyk

Affected Product	**OpenSSL**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-6119)
Description	OpenSSL has released security updates addressing a Denial of Service Vulnerability that exists in their products. **CVE-2024-6119** - Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address resulting in abnormal termination of the application process which can a cause a denial of service. OpenSSL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSSL 3.3, 3.2, 3.1 and 3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://openssl-library.org/news/secadv/20240903.txt

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.