Advisory Alert

Alert Number: AAA20231102 **Date:** November 2, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Command Injection Vulnerability
IBM	**Critical**	Information Disclosure Vulnerability
Redhat	**High**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Dell	**High, Medium**	Multiple Vulnerabilities
Cisco	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Command Injection Vulnerability (CVE-2023-20048)
Description	Cisco has released a security update addressing a Command Injection vulnerability. This vulnerability is due to insufficient authorization of configuration commands that are sent through the web service interface. An attacker could exploit this vulnerability by authenticating to the FMC web services interface and sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute certain configuration commands on the targeted FTD device. Cisco highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco products running a vulnerable release of Cisco FMC Software.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-29MP49hN

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2022-39201)
Description	IBM has released a security update addressing an Information Disclosure Vulnerability, caused by leaking of the authentication cookie in Grafana (Grafana is used by IBM Storage Ceph as part of the dashboard to monitor the stats for each cluster). By sending a specially-crafted request, a remote attacker could exploit this vulnerability to obtain sensitive information and use this information to launch further attacks against the affected system. IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Storage Ceph <6.1 IBM Storage Ceph 5.3z1-z4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7061954

fected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2016-3709, CVE-2022-41723, CVE-2022-48303, CVE-2023-3341, CVE-2023-4527, CVE-2023-4806, CVE-2023-4813, CVE-2023-4911, CVE-2023-34969, CVE-2023-39325, CVE-2023-40217, CVE-2023-44487, CVE-2023-29491, CVE-2023-30630, CVE-2023-38545, CVE-2023-38546)
Description	Redhat has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Denial of service, Sensitive information disclosure, Privilege escalation, Application crash. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Container Native Virtualization 4.13 for RHEL 9 x86_64 Red Hat Container Native Virtualization 4.13 for RHEL 8 x86_64 Red Hat Container Native Virtualization 4.13 for RHEL 7 x86_64 Red Hat Container Native Virtualization for ARM 64 4.13 for RHEL 9 aarch64 Red Hat Container Native Virtualization for ARM 64 4.13 for RHEL 8 aarch64 Red Hat Container Native Virtualization 4.11 for RHEL 8 x86_64 Red Hat Container Native Virtualization 4.11 for RHEL 7 x86_64 Red Hat Container Native Virtualization 4.12 for RHEL 8 x86_64 Red Hat Container Native Virtualization 4.12 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:6235 https://access.redhat.com/errata/RHSA-2023:6251 https://access.redhat.com/errata/RHSA-2023:6248

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-39229, CVE-2022-39306, CVE-2023-0507, CVE-2023-0594, CVE-2022-31123, CVE-2023-22462, CVE-2022-39307, CVE-2022-35957)
Description	IBM has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Privilege escalation, Cross-site scripting, Security restriction bypass, Sensitive information disclosure. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Storage Ceph <6.1 IBM Storage Ceph 5.3z1-z4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7061965 https://www.ibm.com/support/pages/node/7061967 https://www.ibm.com/support/pages/node/7065162 https://www.ibm.com/support/pages/node/7061946 https://www.ibm.com/support/pages/node/7061943 https://www.ibm.com/support/pages/node/7061941 https://www.ibm.com/support/pages/node/7061963 https://www.ibm.com/support/pages/node/7061957

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-43087, CVE-2023-430, 76CVE-2023-29469, CVE-2023-28484, CVE-2023-43076, CVE-2023-3107, CVE-2023-26551, CVE-2023-26552, CVE-2023-26553, CVE-2023-26554, CVE-2022-43551, CVE-2023-23916, CVE-2023-23914, CVE-2023-23915, CVE-2023-27534, CVE-2023-2650, CVE-2023-32461)
Description	Dell has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Information disclosure, Out of memory (OOM) condition, Buffer overflow, privilege Escalation Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000218934/powerscale-onefs-security-updates-for-multiple-security-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000219112/dsa-2023-292-security-update-for-dell-poweredge-server-bios-vulnerability

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20170, CVE-2023-20175, CVE-2023-20195, CVE-2023-20196, CVE-2023-20213, CVE-2023-20244, CVE-2023-20083, CVE-2023-20063, CVE-2023-20155, CVE-2023-20219, CVE-2023-20220, CVE-2023-20095, CVE-2023-20086, CVE-2023-20071, CVE-2023-20177, CVE-2023-20267, CVE-2023-20246, CVE-2023-20070, CVE-2023-20031, CVE-2023-20270, CVE-2023-20005, CVE-2023-20041, CVE-2023-20074, CVE-2023-20206, CVE-2023-20114, CVE-2023-20255, CVE-2023-20042, CVE-2023-20264, CVE-2023-20247, CVE-2023-20245, CVE-2023-20256)
Description	Cisco has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Command injection, Denial of service, Client-Side Request Smuggling, Inspection bypass Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco ISE Release 2.6 and earlier, 2.7, 3, 3.1, 3.2 Cisco FTD Software Release 6.3 and earlier, 6.4, 6.5, 6.6, 6.7, 7, 7.1, 7.2 Cisco ASA Software and FTD Software Cisco Meeting Server Release 3.5 and earlier, 3.6 Cisco Firepower 2100 Series Firewalls running a vulnerable release of Cisco FTD Software Cisco FTD Software with network discovery policy that enables both host and application detection and invokes the Snort 2 Detection Engine Cisco FTD Software or Cisco FMC Software that are configured to allow admin to use expert mode. Cisco FMC Software in the default configuration. ASA Software when it has Cisco AnyConnect Remote Access VPN FTD Software when it has Cisco AnyConnect Remote Access VPN Cisco devices running a Vulnerable release of Cisco FTD Software Cisco ASA Software and FTD Software that was configured for AnyConnect SSL/TLS VPN connections. ASA Software Release 9.18.3 that had remote access VPN configured using SAML 2.0 SSO FTD Software Release 7.2.4 that had had remote access VPN configured using SAML 2.0 SSO
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/publicationListing.x

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.