Advisory Alert

Alert Number: AAA20231116 **Date:** November 16, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple Vulnerabilities
IBM	**High**	Multiple Vulnerabilities
lenovo	**High**	Multiple Vulnerabilities
Juniper	**High**	Multiple Vulnerabilities
Citrix	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3609, CVE-2023-3776, CVE-2023-35001)
Description	Red Hat has released security updates addressing multiple vulnerabilities exists in their products. Successful exploitation of these vulnerabilities could lead to tack-out-of-bounds-read and local privilege escalation. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux Server - AUS 7.6 x86_64 Red Hat Enterprise Linux Server - AUS 7.7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:7243 https://access.redhat.com/errata/RHSA-2023:7294

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44487, CVE-2023-44483)
Description	IBM has released security updates addressing multiple vulnerabilities exists in their products. Successful exploitation of these vulnerabilities could lead denial of service and information disclosure. **CVE-2023-44487-** Denial of service vulnerability caused by a Rapid Reset flaw in the HTTP/2 protocol.A remote attacker could consume excessive server side resources By sending numerous HTTP/2 requests and RST_STREAM frames over multiple streams. **CVE-2023-44483-** Sensitive information disclosure vulnerability caused by the storage of a private key in the log files when using the JSR 105 API. A remote authenticated attacker could exploit this vulnerability to obtain the private key information, and use this information to launch further attacks against the affected system by gaining access to the log files. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM WebSphere Application Server Liberty 17.0.0.3-23.0.0.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7076305 https://www.ibm.com/support/pages/node/7076252

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26345, CVE-2021-46758, CVE-2021-46766, CVE-2021-46774, CVE-2022-23820, CVE-2022-23821, CVE-2022-23830, CVE-2023-20519, CVE-2023-20521, CVE-2023-20526, CVE-2023-20533, CVE-2023-20563, CVE-2023-20565, CVE-2023-20566, CVE-2023-20571, CVE-2023-20592, CVE-2023-20596, CVE-2023-22329, CVE-2023-23583, CVE-2023-25756, CVE-2023-30633, CVE-2023-31100, CVE-2023-34195)
Description	Lenovo has released a security update addressing multiple vulnerabilities exists in their products. Successful exploitation of these vulnerabilities could lead to Arbitrary Code Execution, Denial of Service and Privilege Escalation. Lenovo recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Lenovo Desktop Lenovo Desktop - All in One Lenovo Hyperscale Lenovo Notebook Lenovo Smart Office Lenovo Storage Lenovo ThinkAgile Lenovo ThinkPad Lenovo ThinkServer Lenovo ThinkStation Lenovo ThinkSystem
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-140141

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-22218, CVE-2023-20593, CVE-2023-35788, CVE-2022-44730, CVE-2022-44729, CVE-2023-20900, CVE-2023-3341, CVE-2023-3899, CVE-2023-43057)
Description	Juniper has released security updates to address multiple vulnerabilities in their products. Exploitation of the most severe vulnerabilities could lead to Privilege Escalation, Information Disclosure, Denial of Service, Cross-Site Scripting and Server-Side Request Forgery. Juniper recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Juniper Networks Juniper Secure Analytics: All versions prior to 7.5.0 UP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2023-11-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved?language=en_US

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-23583,CVE-2023-46835)
Description	Citrix has released a security update to address multiple vulnerabilities in the Citrix Hypervisor. Exploiting these vulnerabilities could lead to Privilege Escalation and code execution. Citrix recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Citrix Hypervisor 8.2 CU1 LTSR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX583037/citrix-hypervisor-security-bulletin-for-cve202323583-and-cve202346835

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20240,CVE-2023-20241, CVE-2023-20274, CVE-2023-20208 CVE-2023-20272, CVE-2023-20084, CVE-2023-20265)
Description	Cisco has released security updates to address multiple vulnerabilities in their products. Exploitation of the most severe vulnerabilities could lead to Privilege Escalation, Denial of Service, Arbitrary File Write, Security Bypass and Stored Cross-Site Scripting Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco Secure Client Software Release 5.0 on • Secure Client AnyConnect for Android • Secure Client AnyConnect VPN for iOS • Secure Client (including AnyConnect) for Universal Windows Platform • Secure Client for Linux • Secure Client for MacOS Cisco AppDynamics PHP Agent Release 23.4.0 and earlier Cisco ISE Release 3.0, 3.1, 3.2 Secure Endpoint Connector for Windows Secure Endpoint Private Cloud Cisco IP Phones IP DECT 110 Single-Cell Base Station with Multiplatform Firmware 5.1.2 Cisco IP Phones IP DECT 210 Multi-Cell Base Station with Multiplatform Firmware 5.1.2 Unified IP Phone 6901 running on Cisco Session Initiation Protocol (SIP) Software Release v.9 Unified SIP Phone 3905 running on Cisco Session Initiation Protocol (SIP) Software Release v.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-endpoint-dos-RzOgFKnd https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-j-KxpNynR https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8

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.