Advisory Alert

Alert Number: AAA20231030 **Date:** October 30, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Arbitrary code execution vulnerabilities
Cisco	**Critical**	Privilege Escalation Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
cPanel	**Medium**	Multiple Stored XSS vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary code execution vulnerabilities (CVE-2019-17571, CVE-2022-23307, CVE-2020-9493)
Description	IBM has released a critical security update addressing Arbitrary code execution vulnerabilities in IBM QRadar SIEM. **CVE-2019-17571 -** Arbitrary code execution vulnerability exists in Apache Log4j caused by improper deserialization of untrusted data in SocketServer. A remote attacker could exploit this vulnerability by sending a specially-crafted request. **CVE-2022-23307 -** Arbitrary code execution vulnerability exists in Apache Log4j caused by unsafe deserialization in the in Apache Chainsaw component. A remote attacker could exploit this vulnerability by sending a sending specially-crafted input. **CVE-2020-9493 -** Arbitrary code execution vulnerability exists in Apache Chainsaw caused by unsafe deserialization flaw when reading the log events. An attacker could exploit this vulnerability by sending a specially-crafted request. IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar SIEM7.5 - 7.5.0 UP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7060803

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Privilege Escalation Vulnerabilities (CVE-2023-20198, CVE-2023-20273)
Description	Cisco has released a security remediation to address privilege escalation vulnerabilities in Cisco IOS XE Software. These vulnerabilities may initially allow an attacker to create a local user and password combination. After creating the local account the attacker may elevate privilege to root and write the implant to the file system. Cisco highly recommends to recommends to apply the necessary remediation at your earliest to avoid issues.
Affected Products	Cisco IOS XE Software if the web UI feature is enabled • Cisco IOS XE Software Release Train 17.9 • Cisco IOS XE Software Release Train 17.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-23305, CVE-2022-23302, CVE-2021-4104, CVE-2020-9488, CVE-2023-24329, CVE-2023-43041)
Description	IBM has released security update addressing Multiple Vulnerabilities in their products. Successful exploitation of these vulnerabilities could lead to Arbitrary code execution, sensitive information disclosure or further compromise the system IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar SIEM7.5 - 7.5.0 UP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7060803

Affected Product	**cPanel**
Severity	**Medium**
Affected Vulnerability	Multiple Stored XSS vulnerabilities (CVE-2023-5631, CVE-2023-43770)
Description	Cpanel has released security update addressing Multiple Stored XSS vulnerabilities in Roundcube webmail service versions 1.6.3 and older offered within cPanel & WHM. **CVE-2023-5631-** Roundcube before 1.4.15, 1.5.x before 1.5.5, and 1.6.x before 1.6.4 allows stored XSS via an HTML e-mail message with a crafted SVG document because of rcube_washtml.php behavior. This could allow a remote attacker to load arbitrary JavaScript code **CVE-2023-5631-** Roundcube before 1.4.14, 1.5.x before 1.5.4, and 1.6.x before 1.6.3 allows XSS via text/plain e-mail messages with crafted links because of rcube_string_replacer.php behavior cPanel recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Roundcube versions 1.6.3 and older
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/roundcube-stored-xss-cve-2023-5631-cve-2023-43770/

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.