Advisory Alert

Alert Number: AAA20231219 **Date:** December 19, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Arbitrary Code Execution Vulnerability
Zabbix	**Critical**	Privileges escalation vulnerability
Zimbra	**High**	Multiple Vulnerabilities
IBM	**High** , **Medium** , **Low**	Multiple Vulnerabilities
Zabbix	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2023-46604)
Description	IBM has released security updates addressing Arbitrary Code Execution Vulnerability in Apache ActiveMQ and ActiveMQ Legacy OpenWire Module used in IBM QRadar SIEM. **CVE-2023-46604-** By sending specially crafted request, remote attacker could exploit this vulnerability to execute arbitrary code on the system caused by an unsafe deserialization in the class types in the OpenWire protocol in Apache ActiveMQ and ActiveMQ Legacy. IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar SIEM Versions 7.5 - 7.5.0 UP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7099297

Affected Product	**Zabbix**
Severity	**Critical**
Affected Vulnerability	Privileges escalation vulnerability (CVE-2023-32725)
Description	Zabbix has released a security updates addressing Privileges escalation vulnerability in their products. **CVE-2023-32725-** When an admin user generates a report, a session cookie is created. If this vulnerability is exploited, an attacker could be able to use the session cookie to pretend to be the Zabbix admin user who created the report and authorize himself in the Zabbix frontend with the privileges. Zabbix highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Zabbix server 6.0.0 - 6.0.21 / 6.0.22rc1, 6.4.0 - 6.4.6 / 6.4.7rc1, 7.0.0alpha1 - 7.0.0alpha3 / 7.0.0alpha4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.zabbix.com/browse/ZBX-23854

Affected Product	**Zimbra**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-21930, CVE-2022-21476, CVE-2022-21449, CVE-2023-48432, CVE-2023-50808)
Description	Zimbra has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to data modification, Information disclosure and cross-site scripting. It is recommended by Zimbra to apply the necessary security fixes at earliest to avoid issues.
Affected Products	Zimbra Collaboration Daffodil 10.0.6 Zimbra Collaboration Kepler 9.0.0 Patch 38 Zimbra Collaboration Joule 8.8.15 Patch 45
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.6#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P38#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P45#Security_Fixes

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-26049, CVE-2023-40167, CVE-2023-36479, CVE-2023-32233, CVE-2023-35001, CVE-2023-44487, CVE-2023-42795, CVE-2023-45648, CVE-2023-34040, CVE-2023-22045, CVE-2023-22049, CVE-2023-41835, CVE-2023-36478, CVE-2023-47146, CVE-2023-46589, CVE-2023-40787, CVE-2023-41080)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in IBM QRadar SIEM. If exploited, these vulnerabilities could lead to sensitive information disclosure, HTTP request smuggling, arbitrary code execution, denial of service. It is recommended by IBM to apply the necessary security fixes at earliest to avoid issues.
Affected Products	IBM QRadar SIEM Versions 7.5 - 7.5.0 UP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7099297

Affected Product	**Zabbix**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-32726, CVE-2023-32727, CVE-2023-32728)
Description	Zabbix has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Command Injection and buffer overread. It is recommended by Zabbix to apply the necessary security fixes at earliest to avoid issues.
Affected Products	Zabbix Agent - 5.0.0 - 5.0.39 / 5.0.40, 6.0.0 - 6.0.23 / 6.0.24, 6.4.0 - 6.4.8 / 6.4.9 ,7.0.0alpha1 - 7.0.0alpha6 / 7.0.0alpha8 Zabbix Server- 4.0.0 - 4.0.49 / 4.0.50, 5.0.0 - 5.0.38 / 5.0.39, 6.0.0 - 6.0.22 / 6.0.23rc1, 6.4.0 - 6.4.7 / 6.4.8rc1, 7.0.0alpha0 - 7.0.0alpha6 / 7.0.0alpha7 Agent2 plugin 5.0.0 - 5.0.38 / 5.0.39rc1, 6.0.0 - 6.0.23 / 6.0.24rc1, 6.4.0 - 6.4.8 / 6.4.9rc1, 7.0.0alpha1 - 7.0.0alpha7 / 7.0.0alpha8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.zabbix.com/browse/ZBX-23855 https://support.zabbix.com/browse/ZBX-23857 https://support.zabbix.com/browse/ZBX-23858

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.