Advisory Alert

Alert Number: **AAA20230626** **Date:** **June 26, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**Critical**	Deserialization of untrusted data vulnerability
Ivanti	**High**	Privilege Escalation Vulnerability
Fortinet	**Medium**	Command Injection Vulnerability
IBM	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Deserialization of untrusted data vulnerability (CVE-2023-33299)
Description	Fortinet has released a security update addressing Deserialization of untrusted data vulnerability that exists in FortiNAC.Using specifically crafted requests to the tcp/1050 service, unauthenticated user may be allowed to execute unauthorized code or commands. Fortinet highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	FortiNAC version 9.4.0 through 9.4.2 FortiNAC version 9.2.0 through 9.2.7 FortiNAC version 9.1.0 through 9.1.9 FortiNAC version 7.2.0 through 7.2.1 FortiNAC 8.8 all versions FortiNAC 8.7 all versions FortiNAC 8.6 all versions FortiNAC 8.5 all versions FortiNAC 8.3 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-074

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2023-34298)
Description	Ivanti has released a security update addressing a Privilege Escalation Vulnerability in their products. A Windows user who is logged in can escalate their privileges on the user computer by using the Pulse Secure / Ivanti Secure Access Client or Pulse Secure Installer Service capabilities. ivanti recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ivanti Secure Access Client: before 22.3R3 client version Pulse Secure Installer Service: before 9.1R18.23795 version.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/CVE-2023-34298-Ivanti-Secure-Access-Client-local-privilege-escalation?language=en_US

Affected Product	**Fortinet**
Severity	**Medium**
Affected Vulnerability	Command Injection Vulnerability (CVE-2023-33300)
Description	Fortinet has released a security update addressing a Command Injection Vulnerability in the FortiNAC tcp/5555 service. Using specially crafted input fields, unauthenticated attackers who have sufficient privileges on devices can copy local files on the device to other local directories. Fortinet recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	FortiNAC version 9.4.0 through 9.4.3 FortiNAC version 7.2.0 through 7.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-096

Affected Product	**IBM**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-11087 , CVE-2021-22569 , CVE-2021-22573)
Description	IBM has released security updates addressing Multiple Vulnerabilities in their IBM QRadar SIEM. If exploited theses vulnerabilities could lead to denial of service, sensitive information disclosure and Verification bypass. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	All GoogleCommon versions before 7.5.0-QRADAR-PROTOCOL-GoogleCommon-7.5-20230310180259.noarch.rpm All GoogleCommon versions before 7.4.0-QRADAR-PROTOCOL-GoogleCommon-7.4-20230310180308.noarch.rpm All RabbitMQ versions before PROTOCOL-RabbitMQ-7.5-20230502160719 All AmazonWebServices versions before 7.5.0-QRADAR-PROTOCOL-AmazonWebServices-7.5-20230419193502.noarch.rpm All AmazonWebServices versions before 7.4.0-QRADAR-PROTOCOL-AmazonWebServices-7.4-20230419193457.noarch.rpm
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7006525 https://www.ibm.com/support/pages/node/7006523 https://www.ibm.com/support/pages/node/7006521

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.