Advisory Alert

Alert Number: AAA20240209 **Date:** February 9, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortiguard	**Critical**	Multiple Vulnerabilities
Ivanti	**High**	XXE Vulnerability
Postgresql	**High**	Arbitrary SQL Execution Vulnerability
Fortiguard	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**Fortiguard**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21762, CVE-2024-23113)
Description	Fortiguard has released a security update addressing multiple vulnerabilities that exist in their product **CVE-2024-21762** - Fortiguard has released security update about out-of-bounds write vulnerability in FortiOS may allow a remote unauthenticated attacker to execute arbitrary code or command via specially crafted HTTP requests. **CVE-2024-23113** - Fortiguard has released security update use of externally-controlled format string vulnerability in FortiOS fgfmd daemon may allow a remote unauthentified attacker to execute arbitrary code or commands via specially crafted requests. Fortiguard recommends to apply the necessary software updates to avoid issue
Affected Products	FortiOS 7.4, 7.2, 7.0 FortiOS 6.4, 6.2, 6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-015 https://www.fortiguard.com/psirt/FG-IR-24-029

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	XXE Vulnerability (CVE-2024-22024)
Description	Ivanti has released a security update addressing a XXE Vulnerability that exist in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and ZTA gateways which allows an attacker to access certain restricted resources without authentication. Ivanti recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ivanti Connect Secure (version 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2 and 22.5R1.1) Ivanti Policy Secure version 22.5R1.1 and ZTA version 22.6R1.3.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

Affected Product	**Postgresql**
Severity	**High**
Affected Vulnerability	Arbitrary SQL Execution Vulnerability (CVE-2024-0985)
Description	Postgresql has released a security update addressing an Arbitrary SQL Execution Vulnerability that exists in their products. The attack requires luring the victim into running REFRESH MATERIALIZED VIEW CONCURRENTLY on the attacker's materialized view. As part of exploiting this vulnerability, the attacker creates functions that use CREATE RULE to convert the internally-built temporary table to a view. Postgresql recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Postgresql 12,13,14,15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.postgresql.org/support/security/CVE-2024-0985/

Affected Product	**Fortiguard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-47537, CVE-2023-44487, CVE-2023-26206, CVE-2023-44253,CVE-2023-45581)
Description	Fortiguard has released security updates addressing a Multiple Vulnerabilities that exists in their products. These Vulnerabilities could allow the attacker to cause Man-in-the-Middle, denial of service, cross site scripting, Information disclosure, Execute unauthorized code or commands. Fortiguard recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	FortiOS 7.4, 7.2, 7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-301 https://www.fortiguard.com/psirt/FG-IR-23-397 https://www.fortiguard.com/psirt/FG-IR-23-063 https://www.fortiguard.com/psirt/FG-IR-23-268 https://www.fortiguard.com/psirt/FG-IR-23-357

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.