TLP: WHITE

Advisory Alert

Alert Number: **AAA20240520** **Date:** **May 20, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Zabbix	**Critical**	Time Based SQL Injection Vulnerability
SUSE	**High**	Multiple Vulnerabilities
NETGEAR	**High**	Multiple Vulnerabilities

Description

Affected Product	**Zabbix**
Severity	**Critical**
Affected Vulnerability	Time Based SQL Injection Vulnerability (CVE-2024-22120)
Description	Zabbix has issued a security update addressing a Time Based SQL Injection Vulnerability that exists in Zabbix Server Audit Log. Zabbix server can perform command execution for configured scripts. After command is executed, audit entry is added to "Audit Log". Due to "clientip" field is not sanitized, it is possible to injection SQL into "clientip" and exploit time based blind SQL injection. Zabbix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Zabbix server 6.0.0-6.0.27 Zabbix server 6.4.0-6.4.12 Zabbix server 7.0.0alpha1-7.0.0beta1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.zabbix.com/browse/ZBX-24505

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-48651, CVE-2023-52502, CVE-2023-6546, CVE-2023-6931, CVE-2024-26585, CVE-2024-26610, CVE-2024-26766)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in SUSE Linux kernel. These vulnerabilities could be exploited by malicious users to heap out-of-bounds write, memory corruption, use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241677-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241679-1/

Affected Product	**NETGEAR**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	NETGEAR has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause unauthorized access and multiple security flaws. NETGEAR advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Prosafe Network Management System NMS300 versions before 1.7.0.37
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://kb.netgear.com/000066165/Security-Advisory-for-Missing-Function-Level-Access-Control-on-the-NMS300-PSV-2024-0005 • https://kb.netgear.com/000066164/Security-Advisory-for-Multiple-Vulnerabilities-on-the-NMS300-PSV-2024-0003-PSV-2024-0004

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.