Advisory Alert

Alert Number: AAA20240529 **Date:** May 29, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**Critical**	Security Update
Netgear	**High**	Missing Function Level Access Control Vulnerability
Ivanti	**High**	Privilege Escalation Vulnerability
Red Hat	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities
OpenSSL	Low	Use After Free Vulnerability

Description

Affected Product	**SUSE**
Severity	**Critical**
Affected Vulnerability	Security Update
Description	SUSE has released a security update fixing a regression with nfs (Fix error handling for O_DIRECT write scheduling) that could lead to data corruption. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Real Time 12 SP5 SUSE Linux Enterprise Server 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20241804-1/

Affected Product	**Netgear**
Severity	**High**
Affected Vulnerability	Missing Function Level Access Control Vulnerability
Description	Netgear has released security updates addressing a Missing Function Level Access Control Vulnerability that exists in Prosafe Network Management System (NMS300). Netgear advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NMS300 versions prior to 1.7.0.37
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000066192/Security-Advisory-for-Missing-Function-Level-Access-Control-on-the-NMS300-PSV-2024-0008

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2024-22058)
Description	Ivanti has released security updates addressing a Privilege Escalation Vulnerability that exists in Ivanti Endpoint Manager. Due to a buffer overflow, which could allow a low-privileged user on the local machine that has the EPM Agent installed to execute arbitrary code with elevated permissions. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager (EPM) 2021.1 SU5 and older.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/CVE-2024-22058-Privilege-Escalation-for-Ivanti-Endpoint-Manager-EPM?language=en_US

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3635,CVE-2023-26048,CVE-2023-26049,CVE-2024-1086,CVE-2023-4244,CVE-2023-6240,CVE-2023-6817,CVE-2023-52628,CVE-2024-25742,CVE-2024-25743,CVE-2024-26586)
Description	Red hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, Cookie smuggling, Privilege escalation, Information disclosure. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:3385 • https://access.redhat.com/errata/RHSA-2024:3427 • https://access.redhat.com/errata/RHSA-2024:3421 • https://access.redhat.com/errata/RHSA-2024:3414

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52491, CVE-2023-52618, CVE-2023-52617, CVE-2023-52635, CVE-2023-52486, CVE-2024-26722, CVE-2024-26602, CVE-2023-52489, CVE-2024-26622, CVE-2023-52498, CVE-2024-26702, CVE-2024-26712, CVE-2023-52627, CVE-2023-52494, CVE-2024-26715, CVE-2023-52606, CVE-2024-26685, CVE-2023-47233, CVE-2024-26592, CVE-2023-52595, CVE-2024-26825, CVE-2024-26826, CVE-2023-52608, CVE-2023-52594, CVE-2023-52604, CVE-2023-52637, CVE-2024-26627, CVE-2024-26640, CVE-2024-26808, CVE-2023-52631, CVE-2024-26615, CVE-2024-26717, CVE-2024-26695, CVE-2023-52619, CVE-2024-26910, CVE-2024-26696, CVE-2023-52587, CVE-2024-26916, CVE-2024-26608, CVE-2024-26614, CVE-2023-52633, CVE-2024-26665, CVE-2024-26610, CVE-2023-52598, CVE-2023-52642, CVE-2024-26689, CVE-2024-26606, CVE-2024-26673, CVE-2024-26625, CVE-2024-26636, CVE-2024-26635, CVE-2023-52492, CVE-2024-26600, CVE-2023-52616, CVE-2024-2201, CVE-2024-26698, CVE-2024-26671, CVE-2024-26720, CVE-2023-52622, CVE-2023-52607, CVE-2023-52638, CVE-2023-52530, CVE-2024-26707, CVE-2023-52599, CVE-2023-52614, CVE-2023-52601, CVE-2024-26684, CVE-2024-26704, CVE-2023-52643, CVE-2024-26593, CVE-2024-26664, CVE-2024-26663, CVE-2023-52623, CVE-2024-26679, CVE-2023-52583, CVE-2023-52597, CVE-2024-26676, CVE-2023-52615, CVE-2023-52588, CVE-2023-52435, CVE-2024-26829, CVE-2024-26675, CVE-2024-26920, CVE-2023-52493, CVE-2024-26644, CVE-2023-52602, CVE-2024-26660, CVE-2024-26645, CVE-2024-26594, CVE-2024-23849, CVE-2024-1151, CVE-2024-26641, CVE-2024-26697, CVE-2024-26668)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Denial of service and Sensitive information disclosure. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6795-1

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Use After Free Vulnerabilities (CVE-2024-4741)
Description	OpenSSL has released security updates addressing a Use After Free Vulnerability that exists in their products. This vulnerability is within the SSL_free_buffers fuction which affects applications which directly call this function. OpenSSL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSSL 3.3, 3.2, 3.1, 3.0 and 1.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20240528.txt

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.