Advisory Alert

Alert Number: AAA20230919 **Date:** September 19, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple vulnerabilities
DELL	**High**	Multiple Memory Leak vulnerabilities
Suse	**High**	Kernel Security Updates

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-21216, CVE-2022-33196, CVE-2023-0286)
Description	Red Hat has released a security update for Red Hat Virtualization Host 4.4.z SP 1 in Red Hat Virtualization 4 for Red Hat Enterprise Linux 8. **CVE-2022-21216** - Intel firmware update for insufficient granularity of access control in out-of-band management in some Intel Atom and Intel Xeon Scalable Processors. **CVE-2022-33196 -** Intel firmware update for incorrect default permissions in some memory controller configurations. **CVE-2023-0286** - OpenSSL X.400 address type confusion in X.509 GeneralName. Red Hat recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Red Hat Virtualization 4 for RHEL 8 x86_64 Red Hat Virtualization Host 4 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:5209

Affected Product	**DELL**
Severity	**High**
Affected Vulnerability	Multiple Memory Leak vulnerabilities (CVE-2023-28050, CVE-2023-28027, CVE-2023-28040, CVE-2023-28031, CVE-2023-28060, CVE-2023-28034, CVE-2023-28041, CVE-2023-28028, CVE-2023-28030, CVE-2023-25938, CVE-2023-28033, CVE-2023-28032, CVE-2023-25937, CVE-2023-28044, CVE-2023-28026, CVE-2023-28035, CVE-2023-28058, CVE-2023-28036, CVE-2023-34470)
Description	Dell Technologies has identified multiple memory leak vulnerabilities in the DXE Driver of the PowerEdge T30 and T40 Mini Tower Servers. These vulnerabilities could be exploited by malicious users to compromise affected systems Dell recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	PowerEdge T30 Versions prior to 1.11.0 PowerEdge T40 Versions prior to 1.11.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000214910/dsa-2023-204-security-update-for-dell-poweredge-t30-t40-mini-tower-server-for-multiple-memory-leak-vulnerability

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Kernel Security Updates (CVE-2023-1077, CVE-2023-2156, CVE-2023-3090, CVE-2023-35001, CVE-2022-38457, CVE-2022-40133, CVE-2023-2007, CVE-2023-20588, CVE-2023-34319, CVE-2023-3610, CVE-2023-37453, CVE-2023-3772, CVE-2023-3863, CVE-2023-40283, CVE-2023-4128, CVE-2023-4133, CVE-2023-4134, CVE-2023-4147, CVE-2023-4194, CVE-2023-4273, CVE-2023-4387, CVE-2023-4459, CVE-2023-4569, CVE-2023-2176, CVE-2023-32233, CVE-2023-3567.)
Description	Suse has released security updates addressing Linux Kernel Security updates affecting their products. Exploitation of these vulnerabilities could lead multiple security flows. Suse recommends to apply the necessary security fixes at your earliest to avoid issues
Affected Products	openSUSE Leap 15.4 openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP4 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/2023/suse-su-20233657-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233658-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233659-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233656-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233644-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233647-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233648-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233653-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233629-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233630-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233631-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233632-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233627-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233628-1/

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.