TLP: WHITE

Advisory Alert

Alert Number: AAA20240227 **Date:** February 27, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
F5	**Medium**	Improper Authentication Vulnerability

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51780, CVE-2023-39198, CVE-2023-4921)
Description	Suse has released security updates addressing multiple vulnerabilities. An attacker may exploit these vulnerabilities to cause use-after-free condition, denial of service and privilege escalation. Suse recommends to apply the necessary security updates at your earliest to avoid issues.
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-20240620-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240622-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240624-1/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-42896, CVE-2023-4921, CVE-2023-45871)
Description	Red Hat has issued a security update addressing multiple vulnerabilities that exists in Red Hat Enterprise Linux Server. **CVE-2022-42896** - A use-after-free flaw was found in the Linux kernel's implementation of logical link control and adaptation protocol (L2CAP), part of the Bluetooth stack in the l2cap_connect and l2cap_le_connect_req functions. An attacker with physical access within the range of standard Bluetooth transmission could execute code leaking kernel memory via Bluetooth if within proximity of the victim. **CVE-2023-4921** - A use-after-free flaw was found in qfq_dequeue and agg_dequeue in net/sched/sch_qfq.c in the Traffic Control (QoS) subsystem in the Linux kernel. This issue may allow a local user to crash the system or escalate their privileges on the system. **CVE-2023-45871** - A flaw was found in igb_configure_rx_ring in drivers/net/ethernet/intel/igb/igb_main.c in the IGB driver in the Linux kernel. An overflow of the contents from a packet that is too large will overflow into the kernel's ring buffer, leading to a system integrity issue. Red Hat recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux Server - AUS 7.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0980

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Improper Authentication Vulnerability (CVE-2023-2283)
Description	F5 has released security updates addressing an Improper Authentication vulnerability that exist in their product. The vulnerability exists due to an error within the pki_verify_data_signature() function in pki_crypto.c. The pki_key_check_hash_compatible() function can return SSH_OK value if memory allocation error happens later in the function. A remote attacker can bypass authentication process and gain unauthorized access to the system. F5 recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	BIG-IP Next SPK 1.5.0 - 1.9.1 BIG-IP Next CNF 1.1.0 - 1.2.1 BIG-IP (AFM) 17.1.0 - 17.1.1, 16.1.0 - 16.1.4, 15.1.0 - 15.1.10 Traffix SDC 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000138682

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.