Advisory Alert

Alert Number: **AAA20241206** **Date:** **December 6, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
F5	**High**	Multiple Vulnerabilities
SonicWall	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-3596, CVE-2024-1975, CVE-2023-50387)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-3596** - RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature. **CVE-2024-1975** - If a server hosts a zone containing a "KEY" Resource Record, or a resolver DNSSEC-validates a "KEY" Resource Record from a DNSSEC-signed domain in cache, a client can exhaust resolver CPU resources by sending a stream of SIG(0) signed requests. **CVE-2023-50387** - Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) versions 17.1.0 - 17.1.1, 16.1.0 - 16.1.5 and 15.1.0 - 15.1.10 BIG-IP (APM) versions 17.1.0 - 17.1.1, 16.1.0 - 16.1.5 and 15.1.0 - 15.1.10 BIG-IP (DNS) versions 17.1.0 - 17.1.1, 16.1.0 - 16.1.5 and 15.1.0 - 15.1.10 F5OS-A versions 1.7.0 and 1.5.1 - 1.5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000141008 • https://my.f5.com/manage/s/article/K000140745 • https://my.f5.com/manage/s/article/K000139092

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38475, CVE-2024-40763, CVE-2024-45318, CVE-2024-45319, CVE-2024-53702, CVE-2024-53703)
Description	SonicWall has released security updates addressing multiple vulnerabilities that exist in SonicWall SSL VPN. These vulnerabilities could be exploited by malicious users to cause Path Traversal, Code Execution, Information Disclosure. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SonicWall SSL VPN SMA 100 Series versions 10.2.1.13-72sv and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0018

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause memory leak, memory corruption, out-of-bound, 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, 15.6 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP5, 15-SP6 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5, 15 SP6 SUSE Linux Enterprise Server 12 SP5, 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP5, 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20244217-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244216-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244214-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244210-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244209-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244208-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244207-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244206-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244197-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244195-1/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45590, CVE-2024-28863, CVE-2024-22017, CVE-2023-39332, CVE-2024-21896, CVE-2024-21891, CVE-2024-21890, CVE-2021-36690, CVE-2022-35737, CVE-2023-7104, CVE-2020-8203, CVE-2020-28500, CVE-2021-23337, CVE-2024-39338, CVE-2024-43799, CVE-2024-37071, CVE-2024-45663, CVE-2024-21235)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Privilege Escalation, Permission Bypass, Directory Traversal, Arbitrary Code Execution, Server-Side Request Forgery. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Use Case Manager app versions 1.0.0 - 3.10.0 IBM Db2 versions 10.5.0 - 10.5.11, 11.1.4 - 11.1.4.7, 11.5.0 - 11.5.9 and 12.1 IBM WebSphere Application Server 9.0, 8.5 IBM WebSphere Application Server Liberty - Continuous delivery
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7177981 • https://www.ibm.com/support/pages/node/7175940 • https://www.ibm.com/support/pages/node/7175943 • https://www.ibm.com/support/pages/node/7177984

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.