Advisory Alert

Alert Number: AAA20241011 **Date:** October 11, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
IBM	**High**	Security Update
SonicWall	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
F5	**Medium**	TunnelCrack vulnerability

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell NetWorker vProxy OVA. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetWorker vProxy OVA versions prior to 19.10.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000234730/dsa-2024-422-security-update-for-dell-networker-vproxy-multiple-component-vulnerabilities

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2024-39689)
Description	IBM has released security updates addressing a vulnerability that exists in third party product Certifi, which affects IBM Storage Scale. **CVE-2024-39689** - Certifi python-certifi could provide weaker than expected security, caused by the use of GLOBALTRUST root certificate. An attacker could exploit this vulnerability to launch further attacks on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale versions 5.1.9.0 - 5.1.9.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7172829

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45315, CVE-2024-45316, CVE-2024-45317)
Description	SonicWall has released security updates addressing multiple vulnerabilities that exist in SonicWall SSL-VPN. **CVE-2024-45315** - The Improper link resolution before file access vulnerability in SonicWall Connect Tunnel allows users with standard privileges to create arbitrary folders and files, potentially leading to local Denial of Service (DoS) attack. **CVE-2024-45316** - The Improper link resolution before file access vulnerability in SonicWall Connect Tunnel allows users with standard privileges to delete arbitrary folders and files, potentially leading to local privilege escalation attack. **CVE-2024-45317** - Unauthenticated SMA1000 12.4.x Server-Side Request Forgery (SSRF) Vulnerability allows a remote unauthenticated attacker to cause the server-side application to make requests to an unintended IP address. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SSLVPN SMA 1000 Connect Tunnel Windows (32 and 64-bit) Client 12.4.3.271 and earlier versions SSLVPN SMA 1000 Appliance firmware 12.4.3-02676 and earlier versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0017

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to memory leak, system crash, memory corruption, permission bypass. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.5 openSUSE Leap Micro 5.5 Public Cloud Module 15-SP5 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Availability Extension 15 SP3 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3, 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3,15-SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.5 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5, 15 SP3 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux 15-SP3 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP3, 15 SP5 SUSE Manager Proxy 4.2 SUSE Manager Retail Branch Server 4.2 SUSE Manager Server 4.2 SUSE Real Time Module 15-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243592-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243591-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243587-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243585-1/

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	TunnelCrack vulnerability (CVE-2023-43124)
Description	F5 has released security updates addressing a TunnelCrack vulnerability that exists in BIG-IP APM Clients. **CVE-2023-43124** - BIG-IP APM clients may send IP traffic outside of the VPN tunnel. If a client machine connects to a malicious adjacent network device, such as a router or Wi-Fi hotspot, an attacker may be able to trick the client into sending IP traffic outside of the VPN tunnel. Any clear text traffic leaked outside the tunnel may be accessible to the attacker. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following versions of BIG-IP APM • 17.1.0 - 17.1.1 • 16.1.3.3 - 16.1.4 • 15.1.8 - 15.1.10 • 14.1.5.2 - 14.1.5.6 • 13.1.5.1 APM Clients versions 7.2.3 - 7.2.4 F5 Access for Windows versions 1.2 - 1.3 F5 Access for macOS versions 2.0.2 - 2.0.3 F5 Access for iOS versions 3.0.13 - 3.0.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000136907

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.