Advisory Alert

Alert Number: **AAA20240625** **Date:** **June 25, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Use-after-free Vulnerability
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**	Identity Spoofing Vulnerability
Dell	**High, Medium, Low**	Multiple Vulnerabilities
Hitachi	**Medium**	File and Directory Permissions Vulnerability
SonicWall	**Medium**	Multiple Buffer Overflow Vulnerabilities
WordPress	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell PowerProtect DD series appliances. 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	Data Domain Operating System Versions 7.0 through 7.13 of: • Dell PowerProtect DD series appliances • Dell PowerProtect DD Virtual Edition • Dell APEX Protection Storage Data Domain Operating System and PowerProtect Data Protection Software Versions prior to 2.7.7 of PowerProtect DP Series Appliance – IDPA All Models Data Domain Operating System Versions prior to 5.16.0.0 of PowerProtect Data Manager Appliance model: DM5500 BIOS Versions 7.0 through 7.13 of below Dell PowerProtect DD appliance models • DD6300 • DD6800 • DD9300 Data Domain Operating System Versions 7.0 through 7.13 of Dell PowerProtect DD Management Center Data Domain Operating System Versions 7.8 to 7.13 of Dell PowerProtect DD Management Center with SmartScale feature
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000226148/dsa-2024-219-dell-technologies-powerprotect-dd-security-update-for-multiple-security-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Use-after-free Vulnerability (CVE-2024-1086)
Description	Red Hat has released security updates addressing a Use-after-free Vulnerability that exists in Red Hat Enterprise Linux kernel. **CVE-2024-1086** - A flaw was found in the Netfilter subsystem in the Linux kernel. This issue occurs in the nft_verdict_init() function, allowing positive values as a drop error within the hook verdict, therefore, the nf_hook_slow() function can cause a double-free vulnerability when NF_DROP is issued with a drop error that resembles NF_ACCEPT. The nf_tables component can be exploited to achieve Local Privilege Escalation. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le • Red Hat Enterprise Linux for Power, little endian 7 ppc64le • Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 • Red Hat Enterprise Linux Server - AUS 9.2 x86_64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64 • Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le • Red Hat Enterprise Linux Server 7 x86_64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:4075 • https://access.redhat.com/errata/RHSA-2024:4074 • https://access.redhat.com/errata/RHSA-2024:4073

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 Denial of Service, Data Corruption, Information Disclosure, Use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Availability Extension 12 SP5, 15 SP2, 15 SP3 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP2, 15 SP3 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2, LTSS 15 SP3 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP2, 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Server 12 SP5, 15 SP2, 15 SP3 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux 15-SP2 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux 15-SP3 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP2, 15 SP3 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5 SUSE Manager Proxy 4.1, 4.2 SUSE Manager Retail Branch Server 4.1, 4.2 SUSE Manager Server 4.1, 4.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242185-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242184-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242183-1/

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Identity Spoofing Vulnerability (CVE-2024-37532)
Description	IBM has released security updates addressing an Identity Spoofing Vulnerability that exists in IBM WebSphere products. IBM WebSphere Application Server, which is bundled with IBM WebSphere Hybrid Edition, is vulnerable to identity spoofing and could be exploited by malicious users to compromise the affected system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Hybrid Edition version 5.1 IBM WebSphere Application Server versions 9.0 and 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7158537

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. 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	Precision 7960 Rack BIOS Versions prior to 2.2.7 Precision 7960 XL Rack BIOS Versions prior to 2.2.7 iDRAC9 for 14th Generation PowerEdge Versions prior to 7.00.00.171 iDRAC9 for 15th and 16th Generation PowerEdge Versions prior to 7.10.30.00 Connectrix ED-DCX6-8B Version 9.x through 9.2.0 Connectrix ED-DCX6-4B Version 9.x through 9.2.0 Connectrix ED-DCX7-4B Version 9.x through 9.2.0 Connectrix ED-DCX7-8B Version 9.x through 9.2.0 Connectrix DS-6610B Version 9.x through 9.2.0 Connectrix DS-6620B Version 9.x through 9.2.0 Connectrix DS-6620B-V2 Version 9.x through 9.2.0 Connectrix DS-6630B Version 9.x through 9.2.0 Connectrix DS-6630B-V2 Version 9.x through 9.2.0 Connectrix MP-7810B Version 9.x through 9.2.0 Connectrix DS-7730B Version 9.x through 9.2.0 Connectrix DS-7720B Version 9.x through 9.2.0 Connectrix MP-7850B Version 9.x through 9.2.0 Unisphere for PowerMax Host Installation Versions prior to 10.0.1.5 Unisphere for PowerMax Virtual Appliance Versions prior to 10.0.1.5 Unisphere 360 Host Installation Versions prior to 9.2.4.6 Solutions Enabler Host Installation Versions prior to 10.0.1.1 Solutions Enabler Virtual Appliance Versions prior to 10.0.1.1 eVASA Provider Embedded Versions prior to 10.0.1.469 VASA Provider Standalone Versions prior to 9.2.4.29 PowerMaxOS 5978 Versions prior to 5978.714.714 patch 10081 BIOS Updates: Inspiron 3480 BIOS Versions prior to 1.30.0 Inspiron 3580 BIOS Versions prior to 1.30.0 Latitude 3120 BIOS Versions prior to 1.26.0 Latitude 3190 2-in-1 BIOS Versions prior to 1.34.0 Latitude 3190 BIOS Versions prior to 1.34.0 Latitude 3300 BIOS Versions prior to 1.28.0 Latitude 3310 2-In-1 BIOS Versions prior to 1.24.0 Latitude 3310 BIOS Versions prior to 1.25.0 Latitude 3390 2-in-1 BIOS Versions prior to 1.31.0 Latitude 5288 BIOS Versions prior to 1.36.0 Latitude 5290 2-in-1 BIOS Versions prior to 1.34.0 Latitude 5290 BIOS Versions prior to 1.35.0 Latitude 5300 2-in-1 BIOS Versions prior to 1.31.0 Latitude 5300 BIOS Versions prior to 1.31.0 Latitude 5310 2-in-1 BIOS Versions prior to 1.24.0 Latitude 5310 BIOS Versions prior to 1.24.0 Latitude 5400 BIOS Versions prior to 1.30.0 Latitude 5401 BIOS Versions prior to 1.31.0 Latitude 5410 BIOS Versions prior to 1.28.0 Latitude 5411 BIOS Versions prior to 1.29.0 Latitude 5420 Rugged BIOS Versions prior to 1.32.0 Latitude 5424 Rugged BIOS Versions prior to 1.32.0 Latitude 5480 BIOS Versions prior to 1.36.0 Latitude 5488 BIOS Versions prior to 1.36.0 Latitude 5490 BIOS Versions prior to 1.35.0 Latitude 5491 BIOS Versions prior to 1.33.0 Latitude 5500 BIOS Versions prior to 1.30.0 Latitude 5501 BIOS Versions prior to 1.31.0 Latitude 5510 BIOS Versions prior to 1.28.0 Latitude 5511 BIOS Versions prior to 1.29.0 Latitude 5580 BIOS Versions prior to 1.36.0 Latitude 5590 BIOS Versions prior to 1.35.0 Latitude 5591 BIOS Versions prior to 1.33.0 Latitude 7200 2-In-1 BIOS Versions prior to 1.29.0 Latitude 7210 2-in-1 BIOS Versions prior to 1.30.0 Latitude 7212 Rugged Extreme Tablet BIOS Versions prior to 1.50.0 Latitude 7220 Rugged Extreme BIOS Versions prior to 1.36.0 Latitude 7280 BIOS Versions prior to 1.37.0 Latitude 7290 BIOS Versions prior to 1.38.0 Latitude 7300 BIOS Versions prior to 1.31.0 Latitude 7310 BIOS Versions prior to 1.30.0 Latitude 7380 BIOS Versions prior to 1.37.0 Latitude 7390 2-IN-1 BIOS Versions prior to 1.35.0 Latitude 7390 BIOS Versions prior to 1.38.0 Latitude 7400 2-In-1 BIOS Versions prior to 1.28.0 Latitude 7400 BIOS Versions prior to 1.31.0 Latitude 7410 BIOS Versions prior to 1.30.0 Latitude 7424 Rugged Extreme BIOS Versions prior to 1.32.0 Latitude 7480 BIOS Versions prior to 1.37.0 Latitude 7490 BIOS Versions prior to 1.38.0 Latitude 9410 BIOS Versions prior to 1.29.0 Latitude 9510 2in1 BIOS Versions prior to 1.28.0 Latitude Rugged 7220EX BIOS Versions prior to 1.36.0 Precision 3520 BIOS Versions prior to 1.36.0 Precision 3530 BIOS Versions prior to 1.33.0 Precision 3540 BIOS Versions prior to 1.30.0 Precision 3541 BIOS Versions prior to 1.31.0 Precision 3550 BIOS Versions prior to 1.28.0 Precision 3551 BIOS Versions prior to 1.29.0 Precision 5530 2-In-1 BIOS Versions prior to 1.31.8 Precision 5530 BIOS Versions prior to 1.37.0 Precision 5540 BIOS Versions prior to 1.28.0 Precision 7530 BIOS Versions prior to 1.34.0 Precision 7540 BIOS Versions prior to 1.32.0 Precision 7550 BIOS Versions prior to 1.31.0 Precision 7730 BIOS Versions prior to 1.34.0 Precision 7740 BIOS Versions prior to 1.32.0 Precision 7750 BIOS Versions prior to 1.31.0 Vostro 3480 BIOS Versions prior to 1.30.0 Vostro 3580 BIOS Versions prior to 1.30.0 Vostro 3583 BIOS Versions prior to 1.30.0 Wyse 5470 All-In-One BIOS Versions prior to 1.26.0 Wyse 5470 BIOS Versions prior to 1.25.0 XPS 15 7590 BIOS Versions prior to 1.28.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000223481/dsa-2024-152 • https://www.dell.com/support/kbdoc/en-us/000226356/dsa-2024-286-security-update-for-dell-idrac9-vulnerability • https://www.dell.com/support/kbdoc/en-us/000226365/dsa-2024-214-security-update-for-dell-connectrix-brocade-for-multiple-security-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000215566/dsa-2023-212-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtual-appliance-dell-solutions-enabler-dell-solutions-enabler-virtual-appliance-dell-unisphere-360-dell-vasa-provider-virtual-appliance-and-dell-powermax-embedded-management-sec • https://www.dell.com/support/kbdoc/en-us/000226353/dsa-2024-223-security-update-for-dell-idrac9-vulnerability • https://www.dell.com/support/kbdoc/en-us/000225627/dsa-2024-123

Affected Product	**Hitachi**
Severity	**Medium**
Affected Vulnerability	File and Directory Permissions Vulnerability (CVE-2024-22385)
Description	Hitachi has released security updates addressing a File and Directory Permissions Vulnerability that exists in Hitachi Storage Provider. **CVE-2024-22385** - Incorrect Default Permissions vulnerability in Hitachi Storage Provider for VMware vCenter allows local users to read and write specific files. Hitachi advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Hitachi Storage Provider for VMware vCenter versions 3.1.0 to 3.7.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2024-129/index.html

Affected Product	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Multiple Buffer Overflow Vulnerabilities (CVE-2024-29012, CVE-2024-29013)
Description	SonicWall has released security updates addressing Multiple Buffer Overflow Vulnerabilities that exist in their products. **CVE-2024-29012** - Stack-based buffer overflow vulnerability in the SonicOS HTTP server allows an authenticated remote attacker to cause Denial of Service (DoS) via sscanf function. **CVE-2024-29013** - Heap-based buffer overflow vulnerability in the SonicOS SSL-VPN allows an authenticated remote attacker to cause Denial of Service (DoS) via memcpy function. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	7.1.1 - 7051 and older versions of below Gen7 products • NSa 2700 • NSa 3700 • NSa 4700 • NSa 5700 • NSa 6700 • NSsp 10700 • NSsp 11700 • NSsp 13700 • NSv 270 • NSv 470 • NSv 870 • TZ270 • TZ270W • TZ370 • TZ370W • TZ470 • TZ470W • TZ570 • TZ570P • TZ570W • TZ670
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0008 • https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0009

Affected Product	**WordPress**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	WordPress has released security updates addressing multiple vulnerabilities that exist in WordPress platform. These vulnerabilities could be exploited by malicious users to cause Cross-site Scripting and Path Traversal conditions. WordPress advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WordPress versions prior to 6.5.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wordpress.org/news/2024/06/wordpress-6-5-5/

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.