Advisory Alert

Alert Number: AAA20260703 **Date:** July 3, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
WatchGuard	**Critical**	Use-After-Free vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
WatchGuard	**High**, **Medium**	Multiple Vulnerabilities
F5	**Medium**	Multiple Vulnerabilities
cPanel	**Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**WatchGuard**
Severity	**Critical**
Affected Vulnerability	Use-After-Free vulnerability (CVE-2026-13368)
Description	WatchGuard has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-13368:** WatchGuard Fireware OS contains a race condition leading to a use-after-free vulnerability in LDAP authentication for the Mobile User VPN with IKEv2. A remote unauthenticated attacker could exploit this vulnerability to execute arbitrary code in the context of the iked process on Fireboxes that have a Mobile VPN with IKEv2 configured to use an external LDAP authentication server. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Firebox: • Fireware OS 12.5.x T15 and T35 • Fireware OS 2025.1.x • Fireware OS 12.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00023

Vendor	**Dell**
Severity	**Critical**
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 systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Power Protect Cyber Recovery Software Versions prior to 20.1.0.0 • Dell Cyber Recovery SLES 15 SP4 OS Versions prior to cyber-recovery-osupdate-15.4.0-18.bin • Dell CyberSense 8.17 – SLES 15 SP4 OS Update build 8.17.0-2.0-1 Versions prior to 8.17 • Multiple DD OS Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000483664/dsa-2026-286-security-update-for-dell-powerprotect-cyber-recovery-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000481268/dsa-2026-278-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000475759/dsa-2026-263-security-update-for-dell-cybersense-multiple-third-party-component-vulnerabilities

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43112, CVE-2026-45998, CVE-2026-46209, CVE-2026-46244, CVE-2025-10263, CVE-2026-46316)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Red Hat Enterprise Linux for x86_64 10 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 • Red Hat Enterprise Linux for IBM z Systems 10 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.2 s390x • Red Hat Enterprise Linux for Power, little endian 10 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.2 ppc64le • Red Hat Enterprise Linux for ARM 64 10 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.2 aarch64 • Red Hat CodeReady Linux Builder for x86_64 10 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le • Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 • Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.2 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.2 ppc64le • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.2 s390x • Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.2 aarch64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.2 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.2 s390x • Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.2 ppc64le • Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.2 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64 • Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 10.2 aarch64 • Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 10.2 ppc64le • Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 10.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:34911

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22016, CVE-2026-34282, CVE-2026-22021, CVE-2026-22013, CVE-2026-23865, CVE-2026-22018, CVE-2026-22007, CVE-2026-34268, CVE-2026-20652, CVE-2026-22003, CVE-2024-39286, CVE-2025-31146, CVE-2024-38798, CVE-2025-41226, CVE-2025-41227, CVE-2025-41228, CVE-2025-41241, CVE-2025-41250, CVE-2024-7562)
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 systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NetWorker Runtime Environment (NRE): • Versions prior to 17.0.5 • Version 8.0.28 Dell PowerProtect Data Manager Appliance DM5500 Versions prior to 5.20.1.0 SupportAssist for Home PCs: • Versions prior to 5.0.2.2900 • Versions prior to 5.1.1.3567
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000484594/dsa-2026-269-security-update-for-dell-networker-runtime-environment-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000484391/dsa-2026-282-security-update-for-dell-powerprotect-data-manager-appliance-dm5500-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000484359/dsa-2026-233-security-update-for-dell-supportassist-for-home-pcs-and-dell-supportassist-for-business-pcs-installshield-vulnerability

Vendor	**WatchGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-13053, CVE-2026-13050, CVE-2026-13054, CVE-2026-13079, CVE-2026-8247, CVE-2026-13728, CVE-2026-13084, CVE-2026-13722, CVE-2026-13384, CVE-2026-13383, CVE-2026-13377, CVE-2026-13376, CVE-2026-13375, CVE-2026-13374, CVE-2026-13373, CVE-2026-13371)
Description	WatchGuard has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. WatchGuard advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Firebox: • Fireware OS 12.5.x T15 and T35 • Fireware OS 2025.1.x • Fireware OS 12.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisories

Vendor	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-16775, CVE-2019-16776, CVE-2019-16777)
Description	F5 has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2019-16775:** Versions of the npm CLI prior to 6.13.3 are vulnerable to an Arbitrary File Write. It is possible for packages to create symlinks to files outside of thenode_modules folder through the bin field upon installation. A properly constructed entry in the package.json bin field would allow a package publisher to create a symlink pointing to arbitrary files on a user's system when the package is installed. This behavior is still possible through install scripts. This vulnerability bypasses a user using the --ignore-scripts install option. **CVE-2019-16776:** Versions of the npm CLI prior to 6.13.3 are vulnerable to an Arbitrary File Write. It fails to prevent access to folders outside of the intended node_modules folder through the bin field. A properly constructed entry in the package.json bin field would allow a package publisher to modify and/or gain access to arbitrary files on a user's system when the package is installed. This behavior is still possible through install scripts. This vulnerability bypasses a user using the --ignore-scripts install option. **CVE-2019-16777:** Versions of the npm CLI prior to 6.13.4 are vulnerable to an Arbitrary File Overwrite. It fails to prevent existing globally-installed binaries to be overwritten by other package installations. For example, if a package was installed globally and created a serve binary, any subsequent installs of packages that also create a serve binary would overwrite the previous serve binary. This behavior is still allowed in local installations and also through install scripts. This vulnerability bypasses a user using the --ignore-scripts install option. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP versions: • 17.5.0 - 17.5.1 • 17.1.0 - 17.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000161886

Vendor	**cPanel**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-55956, CVE-2026-55955, CVE-2026-55276, CVE-2026-53434, CVE-2026-53404, CVE-2026-50229)
Description	cPanel has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ea-tomcat101 version 10.1.55 to 10.1.56
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

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.