Advisory Alert

Alert Number: AAA20260618 **Date:** June 18, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
F5	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Improper Access Control Vulnerability
cPanel	**High**, **Medium**	Multiple Vulnerabilities
F5	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
Drupal	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21858, CVE-2023-53372, CVE-2025-40170, CVE-2025-40135, CVE-2025-40158, CVE-2025-68366, CVE-2025-68800, CVE-2025-71089, CVE-2026-23001, CVE-2026-23097, CVE-2026-23191, CVE-2026-23216, CVE-2026-23243, CVE-2026-23392, CVE-2026-31685, CVE-2026-43037, CVE-2026-43038, CVE-2026-43116, CVE-2026-43110, CVE-2026-43163, CVE-2026-43190, CVE-2026-43158, CVE-2026-46243, CVE-2026-46227)
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 - Extended Update Support Extension 8.4 x86_64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:26535

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Dell Data Protection Central Versions 19.10 through 19.12 with Data Protection Central OS Update prior to dpc-osupdate-1.1.27-1 • PowerProtect DP Series (Integrated Data Protection Appliance (IDPA) Appliance Versions prior to 2.7.9 with Data Protection Central OS Update prior to dpc-osupdate-1.1.27-1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000478330/dsa-2026-284-security-update-for-dell-data-protection-central-multiple-third-party-component-vulnerabilities

Vendor	**F5**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42530, CVE-2026-42055)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-42530:** NGINX Open Source has a vulnerability in the ngx_http_v3_module module. When NGINX Open Source is configured to use the HTTP/3 QUIC module, a remote unauthenticated attacker along with conditions beyond their control can use a specially crafted HTTP/3 session to reopen a QPACK encoder stream. This may cause a Use-After-Free in the NGINX worker process, leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. **CVE-2026-42055:** NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_proxy_v2_module and ngx_http_grpc_module modules. This vulnerability exists when the proxy_http_version to 2 or grpc_pass directives are used to proxy HTTP/2 traffic, the ignore_invalid_headers directive is set to off, and the large_client_header_buffers directive size is larger than 2 megabytes. A remote, unauthenticated attacker, along with conditions beyond their control, could send large headers while creating an upstream request. This may cause a heap-based buffer overflow in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NGINX Open Source versions 1.31.0 to 1.31.1 and 1.30.0 to 1.30.2 NGINX Instance Manager version 2.17.0 to 2.22.0 NGINX Gateway Fabric versions 2.0.0 to 2.6.3 and 1.3.0 to 1.6.2 NGINX Ingress Controller versions 5.0.0 to 5.5.0, 4.0.0 to 4.0.1 and 3.5.0 to 3.7.2 NGINX Plus versions 37.0.0 to 37.0.1 and R33 to R36 F5 WAF for NGINX version 5.9.0 to 5.13.1 NGINX App Protect WAF versions 5.2.0 to 5.8.0 and 4.10.0 to 4.16.0 F5 DoS for NGINX version 4.9.0 NGINX App Protect DoS version 4.3.0 to 4.7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000161616 https://my.f5.com/manage/s/article/K000161584

Vendor	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20181, CVE-2026-20190)
Description	Cisco has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-20181:** A vulnerability in Cisco ISE and ISE-PIC could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials. **CVE-2026-20190:** A vulnerability in Cisco ISE and ISE-PIC could allow an unauthenticated, remote attacker to view sensitive information on an affected device. This vulnerability is due to improper authorization checks when a resource is accessed. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to sensitive information, including hashed credentials that could be used in future attacks. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco ISE and Cisco ISE-PIC versions: • Prior to 3.3, 3.3, 3.4 and 3.5[1,2]
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-G5WP8vv

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21858, CVE-2025-68800, CVE-2026-23243, CVE-2026-23392, CVE-2026-43116, CVE-2026-43158, CVE-2026-46243)
Description	Red Hat 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. 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 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:26570 https://access.redhat.com/errata/RHSA-2026:26515

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2026-46461)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-46461:** Dell Server Hardware Manager, versions prior to 3.2.2, contains an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Server Hardware Manager versions prior to 3.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000478484/dsa-2026-243-security-update-for-dell-server-hardware-manager-vulnerability

Vendor	**cPanel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-45447, CVE-2026-34180, CVE-2026-7383, CVE-2026-9076, CVE-2026-42766)
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	EasyApache 4 • ea-openssl11 version 1.1.1w-8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Vendor	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-32682, CVE-2026-11311, CVE-2026-48142)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-32682:** When NGINX Gateway Fabric is configured using GRPCRoutes, an authenticated, remote attacker with permission to create or modify GRPCRoute resources can cause the NGINX Gateway Fabric control plane to terminate by sending undisclosed GRPCRoute configurations containing backendRef filters. **CVE-2026-11311:** When NGINX Plus is configured as the data plane for NGINX Gateway Fabric, an injection vulnerability exists in the NGINX configuration generator component of NGINX Gateway Fabric. User-supplied string values from the NginxProxy Custom Resource Definition serverTokens field and the AuthenticationFilter Custom Resource Definition extraAuthArgs field are rendered directly into NGINX configuration templates without sanitization or escaping. An authenticated attacker with permission to create or modify these Custom Resource Definitions may craft values that inject arbitrary NGINX configuration directives. This is a control plane issue; there is no data plane exposure from the vulnerability trigger itself. **CVE-2026-48142:** NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_charset_module module. When content is served or proxied through a location block with both source_charset utf-8; and a charset directive (for example, charset koi8-r;) configured, remote, unauthenticated attackers can send requests (in conjunction with conditions beyond their control) to cause a heap buffer over-read in the NGINX worker process, leading to limited disclosure of memory or a restart. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NGINX Gateway Fabric versions 2.0.0 to 2.6.3 and 1.3.0 and 1.6.2 NGINX Plus versions 37.0.0 to 37.0.1 and R33 to R36 NGINX Open Source versions 1.31.0 to 1.31.1 and 1.0.0 to 1.30.2 NGINX Instance Manager version 2.17.0 to 2.22.0 F5 WAF for NGINX version 5.9.0 to 5.13.1 NGINX App Protect WAF versions 5.2.0 to 5.8.0 and 4.10.0 to 4.16.0 F5 DoS for NGINX version 4.9.0 NGINX Ingress Controller 5.0.0 to 5.5.0, 4.0.0 to 4.0.1, 3.5.0 to 3.7.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000161786 https://my.f5.com/manage/s/article/K000161611 https://my.f5.com/manage/s/article/K000161585

Vendor	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43284, CVE-2026-46028, CVE-2026-43078, CVE-2026-43077, CVE-2026-43033, CVE-2026-31504, CVE-2026-31431)
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 16.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8390-2 https://ubuntu.com/security/notices/USN-8441-1 https://ubuntu.com/security/notices/USN-8361-3

Vendor	**Drupal**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-55808, CVE-2026-55807, CVE-2026-55806, CVE-2026-55804, CVE-2026-55803)
Description	Drupal 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. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Drupal versions prior to: • 11.3.12 • 11.2.14 • 10.6.11 • 10.5.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2026-009 https://www.drupal.org/sa-core-2026-008 https://www.drupal.org/sa-core-2026-007 https://www.drupal.org/sa-core-2026-006 https://www.drupal.org/sa-core-2026-005

Vendor	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20246, CVE-2026-20220)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-20246:** A vulnerability in the vmadmin CLI of Cisco Umbrella Virtual Appliance could allow an authenticated, local attacker to elevate privileges on an affected device. **CVE-2026-20220:** A vulnerability in the web-based management interface of Cisco Crosswork Network Controller could allow an authenticated, remote attacker to execute arbitrary commands on an affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Umbrella Virtual Appliance Cisco Crosswork Network Controller
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-umbrella-priv-esc-F4wJB7AU • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnc-inj-QNMeEmxk

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.