Advisory Alert

Alert Number: AAA20261029 **Date:** October 29, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Barracuda	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Juniper Networks	**Critical**	Multiple Vulnerabilities
Sophos	**Critical**	Path Traversal Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Cisco	**High**	Multiple Vulnerabilities
Drupal	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Barracuda**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-109618, CVE-2026-109619)
Description	Barracuda has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-109618:** PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE). **CVE-2026-109619:** PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE). Barracuda advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Barracuda Products: • Backup Service Appliance • Firewall Secure Connector • Firewall Insights • SecureEdge
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://trust.barracuda.com/security/php-vulnerabilities

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	Metro Node - Versions prior to 9.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000526631/dsa-2026-466-security-update-for-dell-vplex-multiple-third-party-component-vulnerabilities

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-86350, CVE-2026-76183, CVE-2026-16439, CVE-2026-16441)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• IBM Security Verify Directory Versions - 10.0.0-10.0.4 • IBM Verify Directory Versions - 11.0.0.0 • IBM Db2 Developer Extension Versions - 1.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7294386 • https://www.ibm.com/support/pages/node/7294388 • https://www.ibm.com/support/pages/node/7294412

Vendor	**Juniper Networks**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-103390, CVE-2026-103391, CVE-2026-103392, CVE-2026-103393, CVE-2026-103394, CVE-2026-103400, CVE-2026-103401, CVE-2026-103402, CVE-2026-103403, CVE-2026-103404, CVE-2026-103405, CVE-2026-103406, CVE-2026-103407, CVE-2026-103408, CVE-2026-103409, CVE-2026-103410, CVE-2026-103411, CVE-2026-106079)
Description	Juniper 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. Juniper advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Session Smart Router and Session Smart Conductor - Versions before 7.0.5, 7.1.7, and 7.2.3.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2026-10-On-Demand-Security-Bulletin-Session-Smart-Router-and-Session-Smart-Conductor-Multiple-internally-discovered-vulnerabilities-resolved

Vendor	**Sophos**
Severity	**Critical**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2026-118633)
Description	Sophos has released a security update addressing a vulnerability that exists in their products. **CVE-2026-118633:** A path traversal vulnerability allows a remote unauthenticated attacker to execute arbitrary code as root in Sophos UTM (all versions) after winning a race condition by sustaining repeated attacks for a few minutes when the email proxy is used with scanning enabled. Sophos UTM is end-of-life and the patch must be installed manually. Sophos advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Sophos UTM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.sophos.com/en-us/security-advisories/sophos-sa-20261028-utm-rce

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
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 Platform & Enterprise Software: • JBoss Enterprise Application Platform 8.1 for RHEL 10 (x86_64) • JBoss Enterprise Application Platform 8.1 for RHEL 8 (x86_64) Red Hat Enterprise Linux 8: • Base RHEL 8 (x86_64, ppc64le, s390x, aarch64) • CodeReady Linux Builder 8 (x86_64, ppc64le, aarch64) • 8.4: Advanced Update Support (AUS) (x86_64), Extended Life Cycle Long Life (x86_64) • 8.8: Extended Life Cycle Long Life (x86_64), Update Services for SAP Solutions (ppc64le, x86_64) • 8.10: Extended Life Cycle (all archs) Red Hat Enterprise Linux 9: • Base RHEL 9 (x86_64, ppc64le) • 9.4: Advanced Update Support (AUS) (x86_64), Extended Life Cycle (x86_64, ppc64le), Update Services for SAP Solutions (ppc64le, x86_64) • 9.6: Extended Update Support (x86_64, ppc64le), Advanced Update Support (AUS) (x86_64), Extended Life Cycle (x86_64, ppc64le), Update Services for SAP Solutions (ppc64le, x86_64) • 9.8: Extended Update Support (x86_64, ppc64le), Extended Life Cycle (x86_64, ppc64le), Update Services for SAP Solutions (ppc64le, x86_64) Red Hat Enterprise Linux 10: • Base RHEL 10 (x86_64, ppc64le) • 10.0: Extended Update Support (all archs), CodeReady Linux Builder Extended Update Support (all archs), 4 Years of Updates (all archs) • 10.2: Extended Update Support (x86_64, ppc64le), Extended Life Cycle (x86_64, ppc64le), 4 Years of Updates (x86_64, ppc64le)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:91585 • https://access.redhat.com/errata/RHSA-2026:91638 • https://access.redhat.com/errata/RHSA-2026:91639 • https://access.redhat.com/errata/RHSA-2026:91648 • https://access.redhat.com/errata/RHSA-2026:91650 • https://access.redhat.com/errata/RHSA-2026:92061 • https://access.redhat.com/errata/RHSA-2026:92062 • https://access.redhat.com/errata/RHSA-2026:92063 • https://access.redhat.com/errata/RHSA-2026:92059 • https://access.redhat.com/errata/RHSA-2026:92057 • https://access.redhat.com/errata/RHSA-2026:92209

Vendor	**Dell**
Severity	**High**
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	Connectrix Switches and Directors - Versions prior to 10.0.1 & 10.0.0a1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000526783/dsa-2026-469-security-update-for-dell-connectrix-b-series-fos-and-sannav-vulnerabilities

Vendor	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-111497, CVE-2026-105482, CVE-2026-105483, CVE-2026-106069)
Description	Cisco 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. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Cisco Secure Firewall ASA Software • Cisco Secure FTD Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-oct2026-node-js-Jj3SQ19u

Vendor	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-118563, CVE-2026-118567, CVE-2026-118570)
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 Mobules: • Fasttoggle module Versions prior to 4.1.1 • Bulk Update User Roles module Versions prior to 1.0.5 • CacheFlush Module all Versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2026-283 • https://www.drupal.org/sa-contrib-2026-280 • https://www.drupal.org/sa-contrib-2026-276

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• IBM Security Verify Directory Versions - 10.0.0-10.0.4 • IBM Verify Directory Versions - 11.0.0.0 • IBM Db2 Developer Extension Versions - 1.1.2 • IBM QRadar SIEM Versions - 7.6.0.0 - 7.6.0.5 • IBM QRadar SIEM Versions - 7.5.0 - 7.5.0 UP16 IF02
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7294398 • https://www.ibm.com/support/pages/node/7294412 • https://www.ibm.com/support/pages/node/7294092 • https://www.ibm.com/support/pages/node/7294581 • https://www.ibm.com/support/pages/node/7294580 • https://www.ibm.com/support/pages/node/7294579 • https://www.ibm.com/support/pages/node/7294388 • https://www.ibm.com/support/pages/node/7294387 • https://www.ibm.com/support/pages/node/7294576 • https://www.ibm.com/support/pages/node/7294386 • https://www.ibm.com/support/pages/node/7294582

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.