TLP: WHITE

Advisory Alert

Alert Number: AAA20260521 **Date:** May 21, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Critical**	SQL Injection Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Unauthorized API Access Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2026-9082)
Description	Drupal has released a security update addressing a vulnerability that exists in their product. **CVE-2026-9082**: A vulnerability in this API allows an attacker to send specially crafted requests, resulting in arbitrary SQL injection for sites using PostgreSQL databases. This can lead to information disclosure, and in some cases privilege escalation, remote code execution, or other attacks. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal Core Versions: • 8.9.0 - 10.4.10 • 10.5.0 - 10.5.10 • 10.6.0 - 10.6.9 • 11.0.0 - 11.1.10s • 11.2.0 - 11.2.12 • 11.3.0 - 11.3.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2026-004

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-33815, CVE-2026-33816)
Description	IBM has released a security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-33815:** Package pgproto3, an encoder and decoder of the PostgreSQL wire protocol version 3, is affected by a memory-safety vulnerability in the github.com/jackc/pgx/v5 library. **CVE-2026-33816:** Package pgproto3, an encoder and decoder of the PostgreSQL wire protocol version 3, is affected by a memory-safety vulnerability in the github.com/jackc/pgx/v5 library. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security Verify Access OIDC Provider – Versions 22.09 - 26.03
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7273620

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Unauthorized API Access Vulnerability (CVE-2026-20223)
Description	Cisco has released a security updates addressing a vulnerability that exists in their products. **CVE-2026-20223:** A vulnerability in the access validation of internal REST APIs of Cisco Secure Workload could allow an unauthenticated, remote attacker to access site resources with the privileges of the Site Admin role. This vulnerability is due to insufficient validation and authentication when accessing REST API endpoints. An attacker could exploit this vulnerability if they are able to send a crafted API request to an affected endpoint. A successful exploit could allow the attacker to read sensitive information and make configuration changes across tenant boundaries with the privileges of the Site Admin user. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Secure Workload Cluster Software Versions: • 3.10 • 4.0 • 3.9 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csw-pnbsa-g8WEnuy

ffected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31532, CVE-2026-43284, CVE-2026-46300, and CVE-2026-46333.)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exists in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 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 x86_64 - Extended Life Cycle 9.2 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:19540 https://access.redhat.com/errata/RHSA-2026:19564 https://access.redhat.com/errata/RHSA-2026:19573 https://access.redhat.com/errata/RHSA-2026:19666 https://access.redhat.com/errata/RHSA-2026:19705

ffected Product	**IBM**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-39882, CVE-2026-39883)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-39882:** OpenTelemetry-Go is the Go implementation of OpenTelemetry. Prior to 1.43.0, the otlp HTTP exporters (traces/metrics/logs) read the full HTTP response body into an in-memory bytes.Buffer without a size cap. This is exploitable for memory exhaustion when the configured collector endpoint is attacker-controlled (or a network attacker can mitm the exporter connection). **CVE-2026-39883:** OpenTelemetry-Go is the Go implementation of OpenTelemetry. From 1.15.0 to 1.42.0, the fix for CVE-2026-24051 changed the Darwin ioreg command to use an absolute path but left the BSD kenv command using a bare name, allowing the same PATH hijacking attack on BSD and Solaris platforms. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security Verify Access OIDC Provider – Versions 22.09 - 26.03
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7273620

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20171, CVE-2026-20199)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-20171:** A vulnerability in the Border Gateway Protocol (BGP) enforce-first-as feature of Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, remote attacker to trigger BGP peer flaps, resulting in a denial of service (DoS) condition. This vulnerability is due to incorrect parsing of a transitive BGP attribute. An attacker could exploit this vulnerability by sending a crafted BGP update through an established BGP peer session. If the update propagates to an affected device, it could cause the device to drop the BGP session and flap with the BGP peer that is forwarding this update, resulting in a DoS condition. **CVE-2026-20199:** A vulnerability in the SSL certificate handling of Cisco ThousandEyes Virtual Appliance could allow an authenticated, remote attacker to execute commands on the underlying operating system as the root user. This vulnerability is due to insufficient validation of user-supplied input. An authenticated attacker could exploit this vulnerability by uploading a crafted certificate to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Cisco ThousandEyes Virtual Appliance Cisco Nexus 3000 Series Switches Cisco Nexus 9000 Series Switches in standalone NX-OS mode
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bgp-iefab-3hb2pwtx • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tevacert-rce-RMJVEym5

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.