Advisory Alert

Alert Number: AAA20250814 **Date:** August 14, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Critical**	Authentication Bypass Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Ivanti	**High**, Medium	Multiple Vulnerabilities
HPE	**High**, Medium, Low	Multiple Vulnerabilities
Apache Tomcat	**High**, Low	Multiple Vulnerabilities
Dell	**High**, Low	Multiple Vulnerabilities
F5	Medium	Security Update

Description

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2025-8995)
Description	Drupal has released security updates addressing an Authentication Bypass Vulnerability that exists in Authenticator Login module. **CVE-2025-8995** - The module doesn't sufficiently validate authentication under specific conditions, allowing an attacker to log in as any account where they know the username. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Authenticator Login module versions prior to 2.1.5 for Drupal 10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2025-096

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-48989, CVE-2025-52520)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in JBoss Enterprise Web Server. **CVE-2025-48989** - A flaw was found in Apache Tomcat where malformed client requests can trigger server-side stream resets without triggering abuse counters. This issue, referred to as the "MadeYouReset" attack, allows malicious clients to induce excessive server workload by repeatedly causing server-side stream aborts. While not a protocol bug, this highlights a common implementation weakness that can be exploited to cause a denial of service (DoS). **CVE-2025-52520** - A denial of service flaw was found in Apache Tomcat. For some unlikely configurations of multipart upload, an integer overflow vulnerability may lead to a denial of service via bypassing size limits. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Web Server 6 for RHEL 10 x86_64 JBoss Enterprise Web Server 6 for RHEL 9 x86_64 JBoss Enterprise Web Server 6 for RHEL 8 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:13686 • https://access.redhat.com/errata/RHSA-2025:13685

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-5456, CVE-2025-5462, CVE-2025-5466, CVE-2025-5468)
Description	Ivanti 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 and Information Disclosure. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Connect Secure (ICS) Versions - prior to 22.7R2.7 Ivanti Policy Secure (IPS) Versions - prior to 22.7R1.4 Ivanti ZTA Gateway Versions - 22.8R2.2 Ivanti Neurons for Secure Access Versions - prior to 22.8R1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/August-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-Multiple-CVEs?language=en_US

Affected Product	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31351, CVE-2024-21953, CVE-2024-21965, CVE-2024-21977, CVE-2024-33607, CVE-2024-36331, CVE-2024-36354, CVE-2025-20037, CVE-2025-20044, CVE-2025-20067, CVE-2025-20093, CVE-2025-20109, CVE-2025-21086, CVE-2025-22392, CVE-2025-22836, CVE-2025-22893, CVE-2025-23241, CVE-2025-24296, CVE-2025-24303, CVE-2025-24324, CVE-2025-24325, CVE-2025-24484, CVE-2025-24486, CVE-2025-24511, CVE-2025-25273, CVE-2025-26697, CVE-2025-26863)
Description	HPE 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, Information Disclosure, Privilege Escalation, Arbitrary Code Execution, Unauthorized Data Modification/ Injection. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04930en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04924en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04920en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04912en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04929en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04918en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04915en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04919en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04928en_us&docLocale=en_US

Affected Product	**Apache Tomcat**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-52520, CVE-2025-53506, CVE-2025-48989)
Description	Apache has released security updates addressing multiple vulnerabilities that exist in Apache Tomcat. **CVE-2025-52520** - For some unlikely configurations of multipart upload, an Integer Overflow vulnerability in Apache Tomcat could lead to a DoS via bypassing of size limits. **CVE-2025-53506** - Uncontrolled Resource Consumption vulnerability in Apache Tomcat if an HTTP/2 client did not acknowledge the initial settings frame that reduces the maximum permitted concurrent streams. **CVE-2025-48989** - Tomcat's HTTP/2 implementation was vulnerable to the made you reset attack. The denial of service typically manifested as an OutOfMemoryError. Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache Tomcat versions 11.0.0-M1 to 11.0.8 Apache Tomcat versions 10.1.0-M1 to 10.1.42 Apache Tomcat versions 9.0.0.M1 to 9.0.107
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.10 • https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.44 • https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.108

Affected Product	**Dell**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26383, CVE-2021-46745, CVE-2023-20516, CVE-2023-31326, CVE-2023-31351, CVE-2024-21965, CVE-2024-21977, CVE-2024-33607, CVE-2024-36312, CVE-2024-36331, CVE-2024-36342, CVE-2024-36346, CVE-2024-36354, CVE-2025-0010, CVE-2025-0032, CVE-2025-0034, CVE-2025-20023, CVE-2025-20093, CVE-2025-21086, CVE-2025-22830, CVE-2025-22836, CVE-2025-22839, CVE-2025-22840, CVE-2025-22889, CVE-2025-22893, CVE-2025-23241, CVE-2025-24296, CVE-2025-24303, CVE-2025-24324, CVE-2025-24325, CVE-2025-24484, CVE-2025-24486, CVE-2025-24511, CVE-2025-24515, CVE-2025-24835, CVE-2025-25273, CVE-2025-26697, CVE-2025-26863, CVE-2025-27717, CVE-2025-36581)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000355904/dsa-2025-324-dell-poweredge-server-security-update-for-intel-processors-and-intel-ethernet-controllers-adapters-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000356333/dsa-2025-298-security-update-for-dell-amd-based-poweredge-server-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000356336/dsa-2025-322-security-update-for-dell-amd-based-gpu-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000294953/dsa-2025-129 • https://www.dell.com/support/kbdoc/en-us/000356405/dsa-2025-299-security-update-for-dell-poweredge-server-bios-for-an-access-of-memory-location-after-end-of-buffer-vulnerability

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-54500)
Description	F5 has released security updates addressing a vulnerability that exists in their products. **CVE-2025-54500** - An HTTP/2 implementation flaw allows a denial-of-service (DoS) that uses malformed HTTP/2 control frames to break the maximum concurrent streams limit (HTTP/2 MadeYouReset Attack). This vulnerability allows a remote, unauthenticated attacker to cause an increase in CPU usage that can lead to a DoS on the BIG-IP system. There is no control plane exposure; this is a data plane issue only. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next (all modules) version 20.3.0 BIG-IP Next SPK versions 2.0.0 - 2.0.2 and 1.7.0 - 1.9.2 BIG-IP Next CNF versions 2.0.0 - 2.0.2 and 1.1.0 - 1.4.1 BIG-IP Next for Kubernetes version 2.0.0 BIG-IP (all modules) versions 17.5.0 - 17.5.1, 17.1.0 - 17.1.2, 16.1.0 - 16.1.6 and 15.1.0 - 15.1.10 F5 Silverline (all services)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000152001

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.