# Advisory Alert

**Alert Number:** **AAA20250703** **Date:** **July 3, 2025**

**Document Classification Level** : Public Circulation Permitted | Public

**Information Classification Level** : TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Cisco** | **Critical** | Static SSH Credentials Vulnerability |
| **Ivanti** | **High** | Multiple Vulnerabilities |
| **F5** | **High**, **Medium** | Multiple Vulnerabilities |
| **Citrix** | **Medium** | Denial of Service Vulnerability |
| **Red Hat** | **Medium** | Multiple Vulnerabilities |
| **Cisco** | **Medium** | Multiple Vulnerabilities |
| **Drupal** | **Low** | Access Bypass Vulnerability |

## Description

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **Critical** |
| Affected Vulnerability | Static SSH Credentials Vulnerability (CVE-2025-20309) |
| Description | Cisco has released security update addressing a Static SSH Credentials Vulnerability that exists in their product.<br>**CVE-2025-20309** – A hardcoded root credential vulnerability in Cisco Unified Communications Manager (Unified CM and Unified CM SME) could allow an unauthenticated remote attacker to log in using a built-in root account and execute arbitrary commands as root. This stems from static credentials used during development that cannot be changed or disabled.<br>Cisco advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Cisco Unified Communications Manager (Unified CM) ES builds 15.0.1.13010-1 through 15.0.1.13017-1<br>Cisco Unified Communications Manager Session Management Edition (Unified CM SME) ES builds 15.0.1.13010-1 through 15.0.1.13017-1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssh-m4UBdpE7 |

| | |
|---|---|
| Affected Product | **Ivanti** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-21888, CVE-2024-21893) |
| Description | Ivanti has released security updates addressing multiple vulnerabilities that exist in their products.<br>**CVE-2024-21888** - A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator.<br>**CVE-2024-21893** - A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.<br>Ivanti advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Ivanti Connect Secure — versions 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.2R3, 22.4R2.2, 22.5R1.1 and 22.5R2.2<br>Ivanti Policy Secure — 22.2R3, 22.5R1.1<br>ZTA - version 22.6R1.3 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US |

| | |
|---|---|
| Affected Product | **F5** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-21793, CVE-2016-9063, CVE-2023-24998) |
| Description | F5 has released security updates addressing multiple vulnerabilities that exist in their products.<br>**CVE-2024-21793 -** An OData injection vulnerability in the API endpoint allows an unauthenticated attacker to inject SQL commands. This can lead to data exposure, SQL injection, and potentially arbitrary code execution enabling full compromise of the Central Manager and downstream managed devices<br>**CVE-2016-9063 -** A vulnerability in the Expat XML parser may allow an attacker to trigger an integer overflow when processing specially crafted XML input. This overflow can lead to heap-based buffer overflows, potentially resulting in memory corruption, application crashes, or arbitrary code execution.<br>**CVE-2023-24998 -** Apache Commons FileUpload before 1.5 does not limit the number of request parts to be processed resulting in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads. Note that, like all of the file upload limits, the new configuration option (FileUploadBase#setFileCountMax) is not enabled by default and must be explicitly configured.<br>F5 advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | BIG-IP (DNS) - 17.5.0, 17.1.0 - 17.1.2, 16.1.0 - 16.1.6, 15.1.0 - 15.1.10<br>BIG-IP Next Central Manager - 20.0.1 - 20.1.0<br>BIG-IP (APM) - 17.5.0 - 17.5.1, 17.0.0 - 17.1.2, 16.1.0 - 16.1.6, 15.1.0 - 15.1.10, 14.1.0 - 14.1.5, 13.1.0 - 13.1.5<br>Traffix SDC - 5.2.0, 5.1.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://my.f5.com/manage/s/article/K000138732<br>• https://my.f5.com/manage/s/article/K000139691<br>• https://my.f5.com/manage/s/article/K000133052 |

| | |
|---|---|
| Affected Product | **Citrix** |
| Severity | **Medium** |
| Affected Vulnerability | Denial of Service Vulnerability (CVE-2025-27465) |
| Description | Citrix has released security update addressing a Denial of Service Vulnerability that exists in their product.<br>**CVE-2025-27465** – A vulnerability exists in XenServer 8.4 where improper handling of exceptions during emulation of certain x86 instructions that modify arithmetic flags can cause the hypervisor to crash. Specifically, if the exception metadata is mishandled during replay of these instructions, it may lead to a host-wide denial of service (DoS), affecting all virtual machines running on the host.<br>Citrix advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | XenServer 8.4 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694780&articleURL=XenServer_Security_Update_for_CVE_2025_27465 |

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2022-49395, CVE-2025-21764, CVE-2023-1652, CVE-2022-49407, CVE-2022-4937) |
| 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 affected systems.<br>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64<br>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64, 9.0 x86_64, 8.6 x86_64<br>Red Hat Enterprise Linux Server - AUS 8.6 x86_64, TUS 8.6 x86_64, 8.8 x86_64<br>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le, 8.6 ppc64le |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://access.redhat.com/errata/RHSA-2025:10211<br>• https://access.redhat.com/errata/RHSA-2025:10193<br>• https://access.redhat.com/errata/RHSA-2025:10009 |

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-20310, CVE-2025-20307) |
| Description | Cisco has released security updates addressing multiple vulnerabilities that exist in their products.<br>**CVE-2025-20310**- A stored cross-site scripting vulnerability in Cisco Enterprise Chat and Email (ECE) could allow an authenticated attacker to inject malicious scripts, potentially affecting other users' browsers.<br>**CVE-2025-20307**- An authenticated attacker could exploit a stored XSS flaw in Cisco BroadWorks to execute malicious scripts in the context of another user's browser session.<br>Cisco advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Cisco ECE – 11,12<br>Cisco BroadWorks Application Delivery Platform - Earlier than RI.2025.05 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-xss-CbtKtEYc<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-O696ymRA |

| | |
|---|---|
| Affected Product | **Drupal** |
| Severity | **Low** |
| Affected Vulnerability | Access Bypass Vulnerability (CVE-2025-7030) |
| Description | Drupal has released security update addressing an Access Bypass Vulnerability that exists in their product.<br>**CVE-2025-7030** – A vulnerability in the Enterprise MFA – TFA module for Drupal allows an attacker to bypass authentication by exploiting an alternative access path.<br>Drupal advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Two-factor Authentication (TFA) for Drupal 8.x |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.drupal.org/sa-contrib-2025-085 |

**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.**