TLP: WHITE

Advisory Alert

Alert Number: AAA20241024 **Date:** October 24, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Drupal	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Cisco	**High**, **Medium**, **Low**	Multiple Vulnerabilities
FortiGuard	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20412, CVE-2024-20424, CVE-2024-20329)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-20412** - Due to the presence of static accounts with hard-coded passwords on an affected system, an attacker could log in to the CLI of an affected device with these credentials. A successful exploit could allow the attacker to access the affected system and retrieve sensitive information, perform limited troubleshooting actions, modify some configuration options, or render the device unable to boot to the operating system, requiring a reimage of the device. **CVE-2024-20424** - Due to insufficient input validation of certain HTTP requests, an attacker could authenticate to the web-based management interface of an affected device and then sending a crafted HTTP request to the device. A successful exploit could allow the attacker to execute arbitrary commands with root permissions on the underlying operating system of the Cisco FMC device or to execute commands on managed Cisco Firepower Threat Defense (FTD) devices. To exploit this vulnerability, the attacker would need valid credentials for a user account with at least the role of Security Analyst (Read Only). **CVE-2024-20329** - Due to insufficient validation of user input, an attacker could submit crafted input when executing remote CLI commands over SSH. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Following Cisco products if they are running Cisco FTD Software Release 7.1 through 7.4 with a vulnerability database (VDB) release of 387 or earlier: Firepower 1000 Series Firepower 2100 Series Firepower 3100 Series Firepower 4200 Series • Cisco products if they are running a vulnerable release of Cisco FMC Software, regardless of device configuration. • Cisco products if they are running a vulnerable release of Cisco ASA Software and have the CiscoSSH stack enabled and SSH access allowed on at least one interface. Use Cisco Software Checker to identify vulnerable releases and exposures.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-v3AWDqN7 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssh-rce-gRAuPEUF

Affected Product	**Drupal**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Arbitrary PHP Code Execution, Cross-site Scripting. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Monster Menus 9.3.x - versions 9.3.4 and prior Monster Menus 9.4.x - versions 9.4.0 and above up to 9.4.2 Loft Data Grids module for Drupal 7.x Views SVG Animation for Drupal 10 or 11 versions prior to 1.0.1 SVG Embed for Drupal 7.x versions prior to 1.3 SVG Embed for Drupal 10 or 11 versions prior to 2.1.2 Smartling Connector for Drupal 7.x-4.x versions prior to 7.x-4.19 Smartling Connector for Drupal 7.x-3.x versions prior to 7.x-3.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-052 • https://www.drupal.org/sa-contrib-2024-054 • https://www.drupal.org/sa-contrib-2024-051 • https://www.drupal.org/sa-contrib-2024-050 • https://www.drupal.org/sa-contrib-2024-053

Affected Product	**Cisco**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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 system. Cisco 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://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&impact=high,medium,low&last_published=2024%20Oct&sort=-day_sir&limit=50#~Vulnerabilities

Affected Product	**FortiGuard**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	FortiGuard 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. FortiGuard 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.fortiguard.com/psirt?filter=1&version=&date=2024

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45071, CVE-2024-45072)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM WebSphere Application Server. **CVE-2024-45071** - IBM WebSphere Application Server is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **CVE-2024-45072** - IBM WebSphere Application Server is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A privileged user could exploit this vulnerability to expose sensitive information or consume memory resources. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server versions 9.0 and 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7173270 • https://www.ibm.com/support/pages/node/7173263

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.