Advisory Alert

Alert Number: AAA20231005 **Date:** October 5, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Static Credentials Vulnerability
Cisco	**High**, **Medium**	Multiple Vulnerabilities
Drupal	**Medium**	Access bypass Vulnerability

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Static Credentials Vulnerability (CVE-2023-20101)
Description	Cisco has released security updates addressing Static Credentials Vulnerability that exist in Cisco Emergency Responder product. This vulnerability is due to the presence of static user credentials for the root account that are typically reserved for use during development. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful exploit could allow the attacker to log in to the affected system and execute arbitrary commands as the root user. Cisco recommends to apply the necessary software updates to avoid issue
Affected Products	Cisco Emergency Responder Release 12.5(1)SU4.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cer-priv-esc-B9t3hqk9

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20235, CVE-2023-20259, CVE-2021-1572)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Privilege Escalation, Denial of Service. Cisco recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Catalyst IE3x00 Rugged Series Switches Catalyst IR1100 Rugged Series Routers Catalyst IR1800 Rugged Series Routers Catalyst IR8100 Heavy Duty Series Routers Catalyst IR8300 Rugged Series Routers Embedded Services 3300 Series Switches Cisco NSO Releases 5.4 through 5.4.3.1 Cisco NSO Releases 5.5 through 5.5.2.2 Cisco NSO Releases 5.6 through 5.6.14 Cisco NSO Releases 5.7 through 5.7.12 Cisco NSO Releases 5.8 through 5.8.10 Cisco NSO Releases 6.0 through 6.0.7 Cisco NSO Releases 6.1 through 6.1.3 ConfD Releases 7.4 through 7.4.3 ConfD Releases 7.5 through 7.5.2 ConfD Releases 7.6 through 7.6.14 ConfD Releases 7.7 through 7.7.12 ConfD Releases 7.8 through 7.8.10 ConfD Releases 8.0 through 8.0.7 ConfD Releases 8.1 through 8.1.3 Emergency Responder Prime Collaboration Deployment Unified Communications Manager Unified Communications Manager IM & Presence Service (Unified CM IM&P) Unified Communications Manager Session Management Edition (Unified CM SME) Unity Connection
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rdocker-uATbukKn https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-apidos-PGsDcdNF https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-priv-esc-XXqRtTfT https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-confd-priv-esc-LsGtCRx4

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Access bypass vulnerability
Description	Drupal has released security updates addressing Access bypass vulnerability that exist in the Mail login module. Drupal core contains protection against brute force attacks via a flood control mechanism. This module's functionality did not replicate the flood control, enabling brute force attacks. This module enables users to log in by email address with minimal configurations Drupal recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Mail_login module less than 2.9.0 for Drupal 8 , 9 or 10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2023-048

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.