TLP: WHITE

Advisory Alert

Alert Number: **AAA20240201** **Date:** **February 1, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**High**	Multiple Vulnerabilities
Drupal	**High**	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21888, CVE-2024-21893)
Description	Ivanti has released a security update addressing Authentication Bypass and Command Injection vulnerabilities that exists in Ivanti Connect Secure and Ivanti Policy Secure Gateways. **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. **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. Ivanti recommends to apply the necessary patches at your earliest to avoid issues.
Affected Products	Ivanti Connect Secure and Ivanti Policy Secure Gateways Version 9.x and 22.x
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	**Drupal**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released a security patch update addressing an Access bypass vulnerability in Entity Delete Log Module. The module tracks the deletion of configured entity types, such as node or comments. It does not add sufficient permission to the log report page, allowing an attacker to view information from deleted entities. Drupal recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	Entity Delete Log <1.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-007

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.