مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Security Updates-MISP

Tracking #:432315728

Date:26-03-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that MISP recently released security updates to patch two Vulnerabilities in MISP(Malware Information Sharing Platform).

## TECHNICAL DETAILS:

The Malware Information Sharing Platform (open-source threat intelligence platform) has vulnerabilities that attackers could exploit to compromise systems.

- **CVE-2024-29858-**Improper validation during logo uploads.
  - An attacker could potentially upload malicious code disguised as a logo due to insufficient validation checks within the _uploadLogo function located in app/Controller/OrganisationsController.php
  - Affects MISP software versions before 2.4.187

- **CVE-2024-29859-** NVD assessment not yet provided.
  - Improper checking for a valid file upload in app/Controller/EventsController.php.
  - Affects MISP software versions before 2.4.187

**Fixed Versions:**

- Upgrade MISP to version 2.4.187 or later.

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by MISP.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

1. https://nvd.nist.gov/vuln/detail/CVE-2024-29858
2. https://nvd.nist.gov/vuln/detail/CVE-2024-29859