December 1, 2023

**Overall rating: High**

BRITISH COLUMBIA

**This is a technical bulletin intended for technical audiences.**

## Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability in Cisco Identity Services Engine (ISE). Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to upload malicious files to the web root of the application or conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device.

## Technical Details

A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to upload malicious files to the web root of the application.

This vulnerability is due to insufficient file input validation. An attacker could exploit this vulnerability by uploading a malicious file to the web interface. A successful exploit could allow the attacker to replace files and gain access to sensitive server-side information.

Additionally, a second vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to conduct an XSS attack against a user of the web-based management interface of an affected device.

This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker would need valid administrative credentials.

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit the other vulnerability. In addition, a software release that is affected by one of the vulnerabilities may not be affected by the other vulnerability.

**Exploitability Metrics**
Attack Vector: Network
Attack Complexity: Low
Privileges Required: Low
User Interaction: None

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

## Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

## References

- CVE-2023-20208, CVE-2023-20272

- Cisco Identity Services Engine Vulnerabilities
- VRM Vulnerability Reports