September 13, 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 Fortinet vulnerability. Included were updates for the following:

- FortiADC – multiple versions
- FortiOS – multiple versions
- FortiProxy – multiple versions
- FortiWeb – multiple versions

Technical Details

An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiOS and FortiProxy GUI may allow an authenticated attacker to trigger malicious JavaScript code execution via crafted guest management setting.

Exploitability Metrics
Attack Vector: Local
Attack Complexity: High
Privileges Required: High
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-2023-29183
- Fortinet PSIRT Advisories

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts