October 20, 2023

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a HTTP/2 protocol-level weakness. The vulnerability affects versions OF Business Process Automation, Crosswork Data Gateway, IoT Field Network Director, formerly Connected Grid Network Management System, Prime Infrastructure, Prime Network Registrar, IOx Fog Director, Ultra Cloud Core - Session Management Function, Unified Contact Center Domain Manager (CCDM) and Unified Contact Center Management Portal (CCMP).

Cisco is investigating its product line to determine which products may be affected by this vulnerability and the impact on each affected product. As the investigation progresses, Cisco will update this advisory with information about affected products.

Technical Details

A vulnerability, tracked as CVE-2023-44487, leverages a flaw in HTTP/2 protocol which results in an overload of a targeted web server with malformed requests, allowing malicious actors to launch a DDoS attack targeting HTTP/2 servers.

This attack is called Rapid Reset because it relies on the ability for an endpoint to send a restructured text or RST_STREAM frame immediately after sending a request frame, which makes the other endpoint start working and then rapidly resets the request. The HTTP/2 Rapid Reset attack is simple: The client opens many streams at once as in the standard HTTP/2 attack, but rather than waiting for a response to each request stream from the server or proxy, the client cancels each request immediately. The request is canceled but leaves the HTTP/2 connection open.

The ability to reset streams immediately allows each connection to have an indefinite number of requests in flight. By explicitly canceling the requests, the attacker never exceeds the limit on the number of concurrent open streams. The number of in-flight requests is no longer dependent on the round-trip time, but only on the available network bandwidth.

Open source has reported this vulnerability has been exploited in the wild since August 25, 2023.

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

This vulnerability is rated as a **CRITICAL** 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-2023-44487
- HTTP/2 Rapid Reset Attack Affecting Cisco Products: October 2023
- How it works: The novel HTTP/2 '\'Rapid Reset" attack
- CVE-2023-44487 - HTTP/2 Rapid Reset Attack
- VRM Vulnerability Reports