Recommendations for SolarWinds products and CVE-2023-44487

Security Advisory Summary

If exploited, this HTTP/2 vulnerability allows malicious actors to launch a DDoS attack targeting HTTP/2 servers. The attack sends a set number of HTTP requests using HEADERS followed by RST_STREAM and repeats this pattern to generate a high volume of traffic on the targeted HTTP/2 servers. By packing multiple HEADERS and RST_STREAM frames in a single connection, attackers can cause a significant increase in the request per second and high CPU utilization on the servers that eventually can cause resource exhaustion.

What happened?

This vulnerability has been reported as exploited in the wild in a CISA Notification to cause a denial of service on public-facing servers.

Advisory Details

Severity

7.5 High

Advisory ID

CVE-2023-44487

First Published

10/10/2023

Last Updated

10/20/2023

CVSS Score

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Have there been any reports?

SolarWinds has not received any reports from our customers of attacks related to this vulnerability.

How is SolarWinds addressing this?

See remediations for SolarWinds products below:

What actions should I take?

Any SolarWinds product installed on Microsoft Windows and using IIS can address this issue by following the steps below:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-44487

SolarWinds products using Tomcat:

Web Help Desk (WHD) follow these steps:

- https://support.solarwinds.com/SuccessCenter/s/article/Mitigation-for-HTTP-2-Rapid-Reset-Vulnerability-for-Tomcat-CVE-2023-44487-in-Web-Help-Desk?language=en_US

Database Performance Analyzer (DPA) follow these steps:

- https://support.solarwinds.com/SuccessCenter/s/article/Mitigation-for-HTTP-2-Rapid-Reset-Vulnerability-for-Tomcat-CVE-2023-44487-in-Database-Performance-Analyzer?language=en_US

Security Event Manager (SEM): Per SEM best practices, SolarWinds does not recommend you place the SEM server in a public-facing configuration:

- https://documentation.solarwinds.com/en/success_center/sem/content/install_guide/install-prep/sem-install-preflight.htm