CATO NETWORKS

Sign in

CVE-2025-14213 Socket WebUI: OS Command Injection

0 comments

Follow

Description

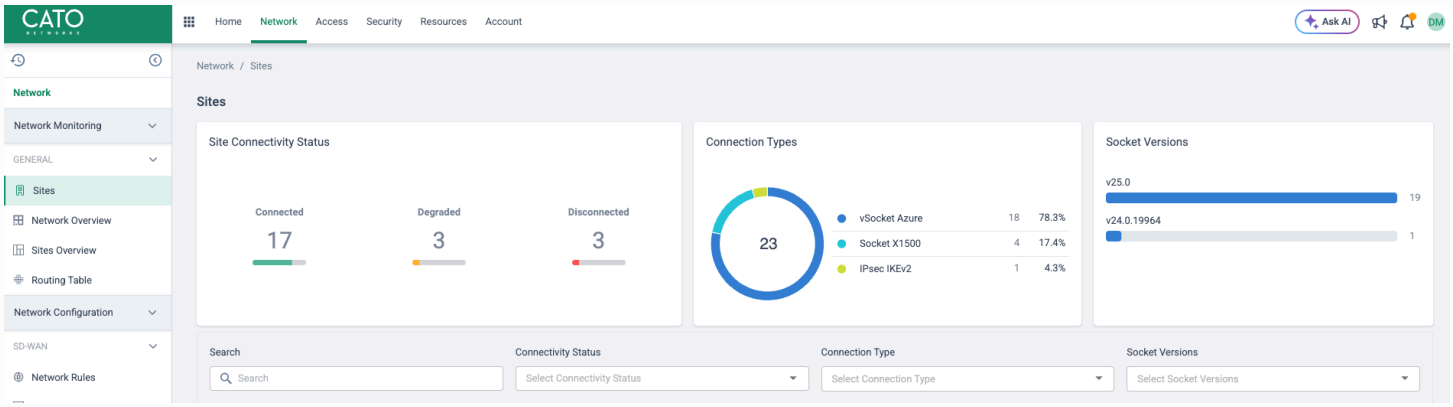
Socket versions lower than v25 contain a command injection vulnerability that allows an authenticated attacker with access to the Socket Web Interface (WebUI) to execute arbitrary operating system commands as the root user on the Socket's internal system.

Severity

The CVSSv4 score is 8.3 (High).

What Changes Do I Need to Make?

From the navigation menu, click **Network** > **Sites**, and check the version of the connected Sockets inside the **Socket Versions** on the right side of the page.



Acknowledgments

Cato Networks thanks the researchers from BugCrowd's bug bounty program for detecting and identifying the issue.

What is the Impact on the Account?

If you don’t upgrade to Socket version 25, the Socket will remain vulnerable. To the best of our knowledge, none of these issues has been exploited in the wild.

Was this article helpful?

0 out of 0 found this helpful

0 comments

Learning Center

Knowledge Base

Getting Started

Home

Network

Access

Security

AI Security

Account

API

Support

Announcements

Community

Cato Cloud Topics

API Topics

Community Help

Partners

Partner CMA Articles

Professional Services Templates and Methodologies

XOps Services

Partner Release Notes

Partner Notifications