

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.

The screenshot shows the Cato Networks management console interface. The navigation menu on the left includes Home, Network, Access, Security, Resources, and Account. The main content area is titled 'Network / Sites' and contains three panels: 'Site Connectivity Status', 'Connection Types', and 'Socket Versions'. The 'Site Connectivity Status' panel shows 17 Connected, 3 Degraded, and 3 Disconnected sites. The 'Connection Types' panel shows a donut chart with 23 total connections, broken down by type: vSocket Azure (18, 78.3%), Socket X1500 (4, 17.4%), and IPsec IKEV2 (1, 4.3%). The 'Socket Versions' panel shows a bar chart with 19 sites on v25.0 and 1 site on v24.0.19964. Below the panels are search and filter controls for Connectivity Status, Connection Type, and Socket Versions.

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





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

