

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Actively Exploited Vulnerability in Brocade Fabric OS
Tracking #:432317145
Date:29-04-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a code injection vulnerability (CVE-2025-1976) affecting Broadcom Brocade Fabric OS versions has been identified and is actively exploited in the wild.

TECHNICAL DETAILS:

A code injection vulnerability (CVE-2025-1976) affecting Broadcom Brocade Fabric OS versions 9.1.0 through 9.1.1d6 has been identified and is actively exploited in the wild. This flaw allows a local user with administrative privileges to execute arbitrary code with root-level access, potentially leading to full system compromise. Immediate action is required to mitigate risks associated with this vulnerability.

Vulnerability Details:

- Vulnerability ID: **CVE-2025-1976**
- CVSS v4.0 Score: 8.6 High
 - Vector: AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- Affected Versions:
 - Brocade Fabric OS 9.1.0 through 9.1.1d6
- Fixed Version:
 - Brocade Fabric OS 9.1.1d7 and later
- Unaffected Versions:
 - Brocade Fabric OS 9.2.0 and later
 - Brocade ASCG and SANnav not affected
- Impact: Local admin users can bypass root access restrictions and execute arbitrary commands or modify the Fabric OS, including adding malicious subroutines.
- Root Cause: Improper validation of IP address input allows code injection

RECOMMENDATIONS:

- Apply Security Updates:
 - Upgrade affected devices to Fixed versions for Fabric OS.
- Access Controls:
 - Limit the number of users with administrative privileges and enforce strict role-based access controls to reduce the attack surface.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25602>