Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

SonicWall SonicOS Flaw Allows Unauthorized Access & Firewall Crashes

Date of Publication	Admiralty Code	TA Number
August 28, 2024	A1	TA2024331

Summary

First Seen: August 2024
Affected Products: SonicWall SonicOS
Impact: SonicWall's SonicOS has been found to have a critical access control vulnerability, identified as CVE-2024-40766, which could allow attackers to gain unauthorized access to resources or cause the firewall to crash. This flaw is characterized as an improper access control bug, highlighting a significant security weakness that needs immediate attention to prevent potential exploitation.

⚙ CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-40766	SonicWall SonicOS Improper Access Control Vulnerability	SonicWall SonicOS	✗	✗	✓

Vulnerability Details

#1 SonicWall has disclosed a critical security vulnerability in its SonicOS management access, identified as CVE-2024-40766. This vulnerability is due to improper access control, potentially allowing unauthorized access to resources and, under certain conditions, causing firewall crashes. Due to the severity of this issue, SonicOS users must take immediate action to mitigate these risks.

#2 CVE-2024-40766 affects a broad range of SonicWall firewall devices, including Gen 5, Gen 6, and Gen 7 devices running SonicOS 7.0.1-5035 and earlier versions. The vulnerability is particularly concerning because it can be exploited over a network without user interaction or authentication, making it a network-based attack vector. The low complexity of the attack makes it easier for attackers to exploit, potentially leading to unauthorized access or firewall crashes.

#3 SonicWall strongly recommends that users update their devices to the latest firmware versions to mitigate the risks associated with CVE-2024-40766. Additionally, to further minimize potential impacts, SonicWall advises restricting firewall management access to trusted sources or disabling firewall WAN management access from internet sources.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-40766	SonicWall SonicOS SOHO (Gen 5) version 5.9.2.14-12o and older, Gen6 Firewalls Version 6.5.4.14-109n and older, Gen7 Firewalls SonicOS build version 7.0.1-5035 and older	cpe:2.3:a:sonicwall:sonicos:*:*:*:*:*:*:*	CWE-284

Recommendations

Update: Users are urged to update to these versions immediately to secure their devices against unauthorized access and potential firewall crashes. SonicWall's SonicOS management access has been addressed in the following firmware versions: SOHO (Gen 5 Firewalls): Version 5.9.2.14-13o
Gen 6 Firewalls: For SM9800, NSsp 12400, and NSsp 12800: Version 6.5.2.8-2n
For other Gen 6 Firewall appliances: Version 6.5.4.15.116n

Regularly Monitor and Audit Access Logs: Keep a close watch on access logs for the firewall management interface to detect any unauthorized access attempts. Regular audits can help identify and mitigate potential security breaches quickly.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0004 Privilege Escalation	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1068 Exploitation for Privilege Escalation	

Patch Details

The critical vulnerability CVE-2024-40766 has been addressed in the following firmware versions. Users of these devices are strongly encouraged to update to the respective firmware versions to mitigate the vulnerability and secure their systems against potential unauthorized access or crashes.

SOHO (Gen 5 Firewalls): Version 5.9.2.14-13o
Gen 6 Firewalls:
For SM9800, NSsp 12400, and NSsp 12800 models: Version 6.5.2.8-2n
For all other Gen 6 Firewall appliances: Version 6.5.4.15.116n

Link: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

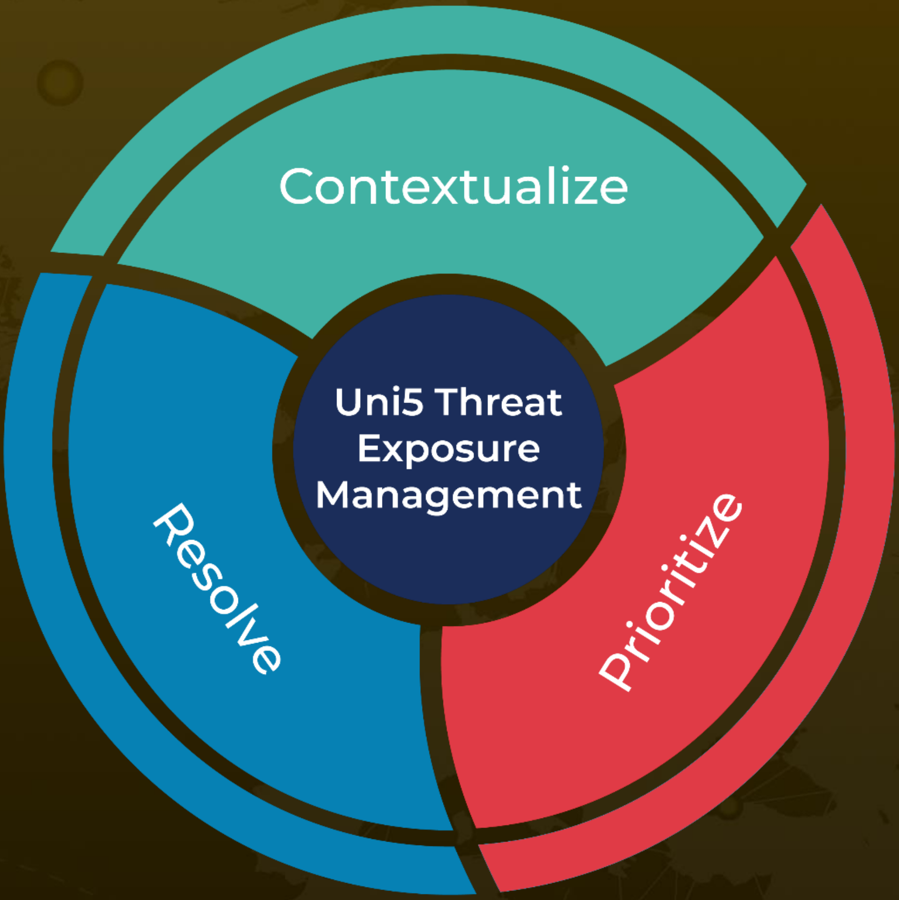
References

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 28, 2024 • 5:30 AM

More at www.hivepro.com