Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

SonicWall SonicOS Flaw Allows Unauthorized Access & Firewall Crashes

Date of Publication	Last Update Date	Admiralty Code	TA Number
August 28, 2024	October 29, 2024	A1	TA2024331

Summary

First Seen: August 2024
Affected Products: SonicWall SonicOS
Malware: Akira and Fog Ransomware
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. Since early August 2024, there has been a notable increase in attacks exploiting this vulnerability, with at least 30 incidents involving Akira and Fog ransomware across various industries.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	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 Since early August 2024, there's been a marked surge in Akira and Fog ransomware attacks, with at least 30 intrusions recorded across various industries. In each case, SonicWall SSL VPNs were exploited early in the attack sequence, and the attacks appear largely opportunistic rather than industry-specific. These incidents are likely tied to CVE-2024-40766, which was suspected to be under active exploitation by September 6, 2024.

#4 Once inside, attackers are encrypting virtual machine storage and exfiltrating sensitive data to increase ransom payment likelihood. These intrusions are also characterized by a rapid transition from initial access to data encryption, leaving defenders with a narrow window for response.

#5 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.

Multi-Factor Authentication (MFA): Implement multi-factor authentication across all user accounts to strengthen access controls. This additional layer of security reduces the risk of unauthorized access, even if passwords are compromised.

Monitor VPN Activity for Anomalies: Use external log monitoring to detect unusual VPN login patterns, such as connections from unexpected locations or hosting providers. Setting up alerts for these events can help identify potential compromises early.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1068 Exploitation for Privilege Escalation	T1078 Valid Accounts

T1078.003 Local Accounts	T1078.002 Domain Accounts	T1586 Compromise Accounts	T1486 Data Encrypted for Impact
T1133 External Remote Services	T1046 Network Service Discovery	T1482 Domain Trust Discovery	T1021 Remote Services
T1021.001 Remote Desktop Protocol	T1021.002 SMB/Windows Admin Shares	T1570 Lateral Tool Transfer	T1555 Credentials from Password Stores
T1003 OS Credential Dumping	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1219 Remote Access Software
T1560 Archive Collected Data	T1560.001 Archive via Utility	T1567 Exfiltration Over Web Service	T1567.002 Exfiltration to Cloud Storage
T1048 Exfiltration Over Alternative Protocol	T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol	T1490 Inhibit System Recovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	7z2407-x64[.]exe, AIPScanner[.]exe, netscan_n[.]exe, adfind[.]exe, sys[.]exe, readme[.]txt, mimikatz[.]exe, 1[.]bat, akira_readme[.]txt, esxi6, .loc
Hostnames	kali, WORKSTATION

TYPE	VALUE
IPv4	77[.]247[.]126[.]158, 208[.]115[.]232[.]194, 184[.]107[.]5[.]46, 66[.]181[.]33[.]32, 185[.]235[.]137[.]150, 45[.]11[.]59[.]16, 79[.]141[.]173[.]238, 57[.]128[.]101[.]78, 194[.]33[.]45[.]167, 23[.]227[.]162[.]18, 45[.]86[.]208[.]146
SHA1	3477a173e2c1005a81d042802ab0f22cc12a4d55, 86233a285363c2a6863bf642deab7e20f062b8eb, ce4758849b53af582d2d8a1bc0db20683e139fcc, 67396e1aacacb6efbca51f4c03d2017af78c9842, 806a232379ad0af437d4bc5b87fb42065dbf82d4, e6b34a589e61b155ab70f11f8f7393316c9a3189, 1d345799307c9436698245e7383914b3a187f1ec, ce8de59e2277e9003f3a9c96260ce099ca7cda6c, 15035d9f218a4629a8449829eba85b40806f4f59, 7931b85054c29be4cc3c9250a5dc4a821a44604, c26cfb9f9910fe585630940a777022702257548d, 8ea2bf726044e98479076d0e64327f7ae7a6e5f2, 99ed6135defff6e675d626f742389d6280abdb60, c1f271e5ced7a5badf62042ab882584e45aeab37, 8e81daa8c88a1e40c60332917c4ad5fa57acbb23, 75d7d147f66004c7131ad0d0fa5603451be45ba, f5ca50ee8bc9d01760c7d0d4fc0c814cbbf26bc9, 03f193a9385cf8fe2429e14aab4862b1627ff9d5, 57aed4cf2972b51e0a7d37e9ca0c4b1b6985e1f1, 2aab7f60262db7589d83fd7d13c968a6b93f75b9, e7fb4bf69be5ac4583c0c02e26a17bd3cdef4c02, 6ae600ccff0741ce420bbd372c931b951094121f, c144446dc23c86c7c9b26ce87c3176866372f6d1, 363068731e87bcee19ad5cb802e14f9248465d3
AS Number	AS29802, AS43641, AS58061, AS59711, AS62240, AS202015, AS395092, AS64236, AS32613

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

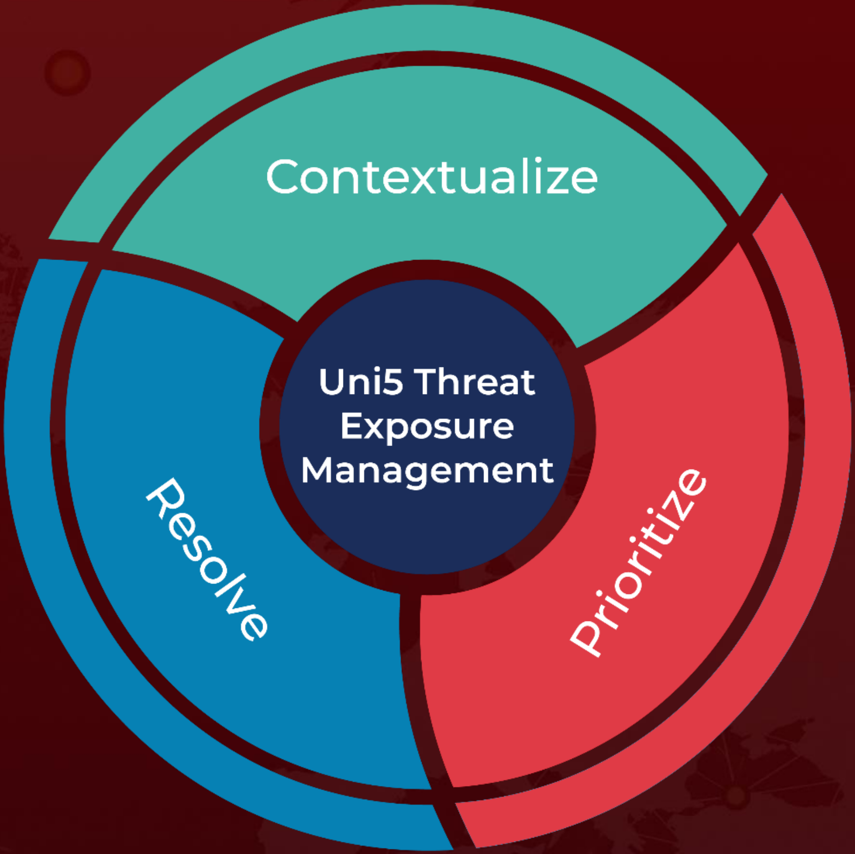
https://arcticwolf.com/resources/blog/arctic-wolf-observes-akira-ransomware-campaign-targeting-sonicwall-sslvpn-accounts/

https://arcticwolf.com/resources/blog/arctic-wolf-labs-observes-increased-fog-and-akira-ransomware-activity-linked-to-sonicwall-ssl-vpn/

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