Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Over 5,000 SonicWall Firewalls Still Vulnerable to CVE-2024-53704 Exploit

Date of Publication	Admiralty Code	TA Number
February 13, 2025	A1	TA2025039

Summary

First Seen: November 5, 2024
Affected Products: SonicWALL NSv devices, SonicWall SSLVPN
Impact: A critical security flaw has been discovered in the SSLVPN authentication mechanism of SonicWall NSv devices and select firewall models. Tracked as CVE-2024-53704, this vulnerability allows remote attackers to bypass authentication, potentially resulting in unauthorized access. With proof-of-concept (PoC) exploits now publicly available, the risk of active exploitation is greater. Immediate patching is essential to prevent potential breaches.

⚙ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-53704	SonicWall SonicOS SSLVPN Improper Authentication Vulnerability	SonicWALL NSv devices, SonicWall SSLVPN	✗	✓	✓

Vulnerability Details

#1 A critical vulnerability, CVE-2024-53704, has been discovered in the SSL VPN component of certain SonicWall firewalls, allowing remote attackers to bypass authentication and hijack active VPN sessions without valid credentials.

#2 The issue stems from improper handling of Base64-encoded session cookies, caused by a flawed authentication algorithm. Exploiting this vulnerability allows attackers to gain unauthorized access to the system. Once exploited, attackers can access Virtual Office bookmarks, retrieve NetExtender client configuration profiles, establish VPN tunnels, and infiltrate private networks linked to the victim’s account.

#3 SonicWall released patches addressing this vulnerability on January 7, 2025. Despite this, as of early February 2025, over 5,000 SonicWall firewalls remained unpatched and vulnerable.

#4 The attack involves sending a specially crafted session cookie containing a base64-encoded null-byte string to the SSL VPN authentication endpoint (/cgi-bin/sslvpnclient). This triggers a validation flaw, causing the system to accept the attacker's request as a legitimate session, logging out the actual user and granting the attacker full access.

#5 With this level of control, attackers can exfiltrate VPN client settings, establish unauthorized VPN connections, and move laterally within compromised networks. The situation has escalated further with the public release of proof-of-concept (PoC) exploit code, significantly lowering the barrier for attackers to weaponize this flaw. SonicWall users must immediately patch their devices to prevent active threats.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-53704	SonicWALL Gen7 NSv Version Prior to 7.0.1-5165, SonicWALL Gen7 Firewalls Version Prior to 7.1.3-7015, SonicWALL TZ80 Version Prior to 8.0.0-8037	cpe:2.3:o:sonicwall:sonicos:*:*:*:*:*:*:*:*	CWE-287

Recommendations

Apply Patches Immediately: Ensure all affected SonicWall firewalls are updated to the latest firmware versions 7.1.x and 8.0.0 to fix CVE-2024-53704. Regularly monitor for firmware updates and apply them as soon as they become available. If immediate patching isn't possible, temporarily disable SSL VPN access or restrict it to trusted IPs to reduce the risk of exploitation.

Monitor for Exploitation Attempts: Regularly review VPN logs for any signs of suspicious activity, such as unusual login attempts, unexpected session terminations, or unauthorized connections. Additionally, configure intrusion detection rules to flag requests targeting the /cgi-bin/sslvpnclient endpoint, as attackers may attempt to exploit this vulnerability to bypass authentication.

Revoke and Reset Compromised Sessions: Immediately invalidate all active SSL VPN sessions to prevent unauthorized access and require all users to re-authenticate. Additionally, reset VPN credentials for all accounts and consider enforcing multi-factor authentication (MFA) to add an extra layer of security against unauthorized logins.

Restrict SSH Access: To minimize the risk associated with this SSH vulnerability, limit firewall management access to trusted IP addresses or disable SSH access from the internet entirely. This reduces the attack surface and helps prevent unauthorized access attempts.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0003** Persistence	**TA0004** Privilege Escalation
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1588.005** Exploits	**T1190** Exploit Public-Facing Application
T1556 Modify Authentication Process	**T1133** External Remote Services	**T1068** Exploitation for Privilege Escalation	

Patch Details

Update the SonicWALL firewalls to the latest versions.
SonicWALL Gen7 NSv – Update to Version 7.0.1-5165 and higher
SonicWALL Gen7 Firewalls – Update to Version 7.1.3-7015 and higher
SonicWALL TZ80 – Update to Version 8.0.0-8037 and higher

Links: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003

References

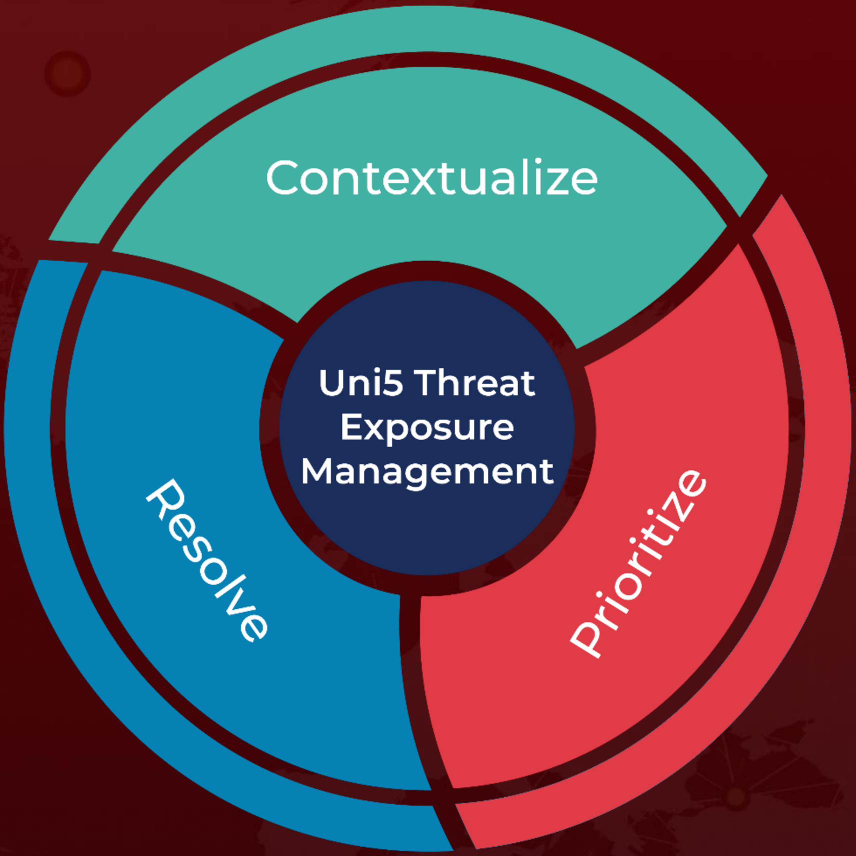
https://bishopfox.com/blog/sonicwall-cve-2024-53704-ssl-vpn-session-hijacking

https://www.zerodayinitiative.com/advisories/ZDI-25-012/

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

February 13, 2025 • 6:50 AM

More at www.hivepro.com