مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – SonicWall

Tracking #:432316066

Date:19-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that SonicWall released security updates to address vulnerabilities in their products.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-29014** | CVSS v3: 7.1 – Medium
  - Vulnerability in SonicWall NetExtender Windows (32 and 64-bit) client 10.2.339 and earlier versions allows an attacker to arbitrary code execution when processing an EPC Client update.

- **CVE-2024-40764** | CVSS v3: 7.5– Medium
  - Heap-based buffer overflow vulnerability in the SonicOS IPSec allows an unauthenticated remote attacker to cause Denial of Service (DoS).

Affected versions:

- NetExtender Windows (32 and 64 bit) 10.2.339 and earlier versions.
- Gen6 NSv - NSv10, NSv25, NSv50, NSv100, NSv200, NSv300, NSv400, NSv800, NSv1600 - 6.5.4.4-44v-21-2395 and older versions
- Gen7 - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700 NSv 270, NSv 470, NSv 870 - 7.0.1-5151 and older versions, 7.1.1-7051 and older versions

Fixed versions:

- NetExtender Windows (32 and 64 bit) 10.2.341 and higher versions.
- Gen6 6.5.4.v-21s-RC2457
- Gen7 7.0.1-5161, 7.1.1-7058, 7.1.2-7019

Note: NetExtender Linux client versions are not affected by this vulnerability.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by SonicWall.

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://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0011
- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0012