مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – SonicWall

Tracking #:432316391

Date:14-10-2024

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

SonicWALL has identified several vulnerabilities in the SMA1000 Connect Tunnel Windows Client and SMA1000 Appliance firmware. These vulnerabilities could potentially allow attackers to execute denial-of-service (DoS) attacks or escalate privileges.

Vulnerabilities Details:

1. **CVE-2024-45315 - Denial-of-Service Vulnerability:**
    - Improper link resolution before file access could allow users with standard privileges to create arbitrary folders and files, potentially leading to a local DoS attack.
    - **CVSS Score:** 6.1
2. **CVE-2024-45316 - Local Privilege Escalation Vulnerability:**
    - Improper link resolution before file access could allow users with standard privileges to delete arbitrary folders and files, potentially leading to local privilege escalation.
    - **CVSS Score:** 7.8
3. **CVE-2024-45317 - Server-Side Request Forgery (SSRF) Vulnerability:**
    - Unauthenticated SSRF vulnerability could allow a remote attacker to cause the server-side application to make requests to an unintended IP address.
    - **CVSS Score:** 7.2

Affected Products and Versions:

- **SMA1000 Connect Tunnel Windows (32 and 64-bit) Client:** 12.4.3.271 and earlier versions
- **SMA1000 Appliance Firmware:** 12.4.3-02676 and earlier versions

Fixed Versions:

- **SMA1000 Connect Tunnel Windows (32 and 64-bit) Client:** version 12.4.3.281 or later.
- SMA1000 Platform Hotfix - 12.4.3-02758

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-2024-0017