Security Advisory 2021-006

SonicWall 0-day Vulnerabilities

February 4, 2021 — v1.1

TLP:WHITE

History:

- *02/02/2021 — v1.0 – Initial publication*
- *04/02/2021 — v1.1 – Update with info about a patch and possible IoCs*

Summary

On January 22nd, SonicWall has disclosed that it has been hacked in an attack that exploited zero-day vulnerabilities in several of its own VPN software products, SMA 100 series [1, 2]. On February 3rd, SonicWall has released a new firmware update that fixes the vulnerability [4].

Technical Details

On January 22nd, the manufacturer informed that faced a *coordinated attack* with unknown actors leveraged zero-day vulnerabilities in SonicWall products to target its internal systems [1, 3]. They said that the attack was carried out by *highly sophisticated threat actors* but has not released any information on the identity of the assailants.

The vulnerability results in improper SQL command neutralisation in the SonicWall SSLVPN SMA100 product and allows remote exploitation for credential access by an unauthenticated attacker [5].

Affected Products

This vulnerability affects SMA100 build version 10.x [5]:

- Physical Appliances: SMA 200, SMA 210, SMA 400, SMA 410
- Virtual Appliances: SMA 500v (Azure, AWS, ESXi, HyperV)

Recommendations

CERT-EU strongly recommends to upgrade your affected appliance(s) to the last version of the firmware (SMA 10.2.0.5-29sv) [6, 7].

Moreover, CERT-EU recommends to take the following actions:

- Reset the passwords for any users who may have logged in to the device via the web interface.
- Enable multi-factor authentication (MFA).

Admins who cannot immediately apply this patch should enable the Web Application Firewall (WAF) until they are ready to deploy the patch on affected devices.

Hunting for Compromise

NCC Group shared some guidance on how to look for potential indicators of compromise [4]. Administrators could look for requests to `/cgi-bin/management` that do not have a previous successful request to `/__api__/v1/logon` or `/__api__/v1/logon//authenticate`. If these requests do exist, then it would indicate an authorisation bypass to the management interface.

To check for user-level bypass via the VPN client or the web, administrators should look for access log entries to:

```
/cgi-bin/sslvpnclient
/cgi-bin/portal
```

If a user accessed these paths without also previously accessing the following paths, it indicates a *user-level* authorisation bypass.

Via VPN client:

```
/cgi-bin/userLogin (for VPN client)
```

Via web:

```
/__api__/v1/logon (200)
/__api__/v1/logon//authenticate
```

References

[1] https://www.sonicwall.com/support/product-notification/urgent-security-notice-probable-sma-100-series-vulnerability-updated-jan-27-2021/210122173415410/

[2] https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001

[3] https://portswigger.net/daily-swig/sonicwall-updates-users-after-highly-sophisticated-cyber-attack-leverages-zero-day-vulnerabilities

[4] https://www.bleepingcomputer.com/news/security/sonicwall-fixes-actively-exploited-sma-100-zero-day-vulnerability/

[5] https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001

[6] https://www.sonicwall.com/support/knowledge-base/how-to-upgrade-firmware-on-sma-100-series-appliances/170502339501169/#:~:text=Now%20from%20the%20Web%20UI,new%20version%20in%20New%20Firmware.

[7] https://www.sonicwall.com/support/knowledge-base/smb-ssl-vpn-upgrading-firmware-on-sma-500v-virtual-appliance/170502851052498/