PUSAT OPERASI KEAMANAN SIBER NASIONAL

IMBAUAN KEAMANAN
KERENTANAN *ZERO-DAY* PADA PRODUK *SECURE MOBILE ACCESS* (SMA) MILIK SONICWALL

Ringkasan Kerentanan

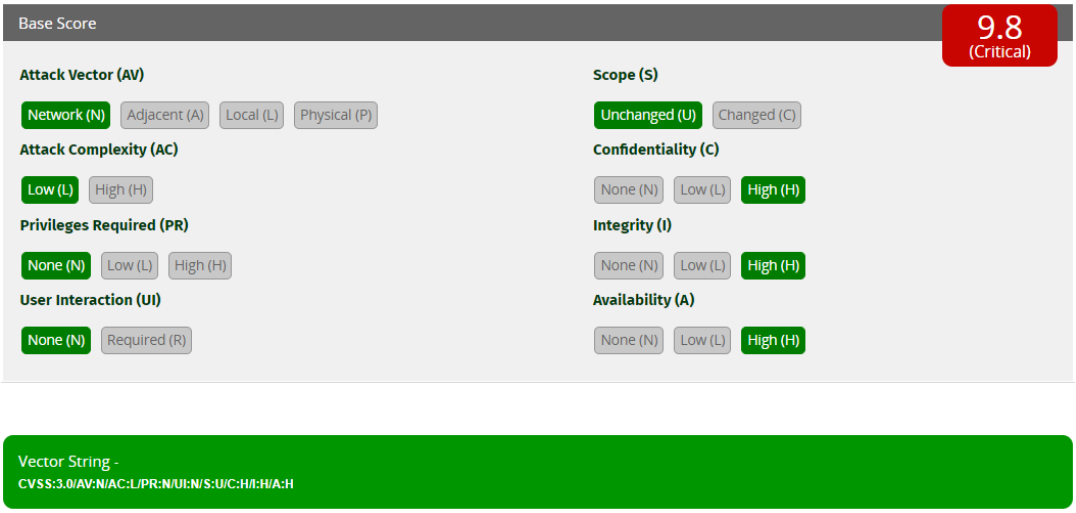
- SonicWall mengonfirmasi adanya kerentanan *zero-day* (CVE-2021-20016) dalam produk SMA Seri 100 dengan versi firmware 10.x, diantaranya SMA 200, SMA 210, SMA 400, SMA 410 dan SMA 500v.
- Kerentanan ini memungkinkan terjadinya eksploitasi yang dilakukan oleh penyerang tidak terautentikasi dalam melakukan kueri SQL berupa *username*, *password*, dan informasi kredensial lainnya.
- Kerentanan ini memiliki nilai kerentanan sebesar 9.8 yang termasuk ke dalam kategori **KRITIKAL**.
- Diharapkan kepada administrator dan pengguna SonicWall agar melakukan pembaruan keamanan, mengatur ulang kata sandi untuk semua pengguna, dan mengaktifkan *multifactor authentication* (MFA) sebagai tindakan memitigasi kerentanan ini.

Pendahuluan

SonicWall kembali memberikan peringatan terkait adanya kerentanan *zero-day* (CVE-2021-20016). Sebelumnya SonicWall telah memberikan pemberitahuan pertama terkait kerentanan ini pada tanggal 25 Januari 2021. Pada pembaruan keamanan pertama disebutkan SonicWall telah melakukan pembaruan pada semua produk SMA seri 100, sementara produk lainnya tidak terpengaruh dengan kerentanan sebelumnya. Pada peringatan kedua ini, kerentanan terdapat pada kode produk SMA seri 100 dengan firmware versi 10.x. Kerentanan disebabkan karena proses Netralisasi perintah SQL yang tidak tepat. Eksploitasi yang berhasil dilakukan dapat mengizinkan penyerang tidak terautentikasi untuk mengakses *username, password,* dan kredensial lainnya.

Nilai Kerentanan

Berdasarkan CVSS v3.x versi NIST, kerentanan ini memiliki nilai 9.8 dan dikategorikan **KRITIKAL**. Saat ini, SonicWall juga sedang melakukan penelusuran lebih lanjut mengenai produk SMA seri 100 yang terdampak.



Gambar 1. *Base Score* untuk kerentanan *zero-day* (CVE-2021-20016) dengan Vector String (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Versi Terdampak

Kerentanan *zero-day* ini berdampak pada produk SMA Seri 100 dengan versi firmware 10.x dengan rincian sebagai berikut:

Tabel 1. Versi SMA yang terkena dampat kerentanan *zero-day*

Affected Devices	***Apliance Type***
SMA 200	*Physical*
SMA 210	*Physical*
SMA 400	*Physical*
SMA 410	*Physical*
SMA 500v	*Virtual* (Azure, AWS, ESXi, HyperV)

Sumber: (https://www.tenable.com/blog/cve-2021-20016-zero-day-vulnerability-in-sonicwall-secure-mobile-access-sma-exploited)

Sementara pada produk SMA seri 100 sebelum firmware versi 10.x tidak terpengaruh terhadap kerentanan ini. Akan tetapi, SonicWall menyarankan kepada administrator yang produknya terpengaruh untuk melakukan *patching* (SMA 10.2.0.5-29sv) dengan segera. Setelah menerapkan pembaruan keamanan, administrator disarankan untuk mengatur ulang kata sandi seluruh pengguna dan mengaktifkan *multifactor authentication* (MFA) sebagai langkah dalam meningkatkan keamanan.

Panduan Mitigasi Kerentanan

Pengguna yang terdampak oleh kerentanan ini disarankan untuk melakukan langkah mitigasi sebagai berikut:

1. **Memperbarui firmware SMA ke versi 10.2.0.5-29sv yang tersedia di www.mysonicwall.com.**

   Panduan dapat dibaca di https://www.sonicwall.com/support/knowledge-base/how-to-upgrade-firmware-on-sma-100-series-appliances/170502339501169/ dan https://www.sonicwall.com/support/knowledge-base/smb-ssl-vpn-upgrading-firmware-on-sma-500v-virtual-appliance/170502851052498/.

2. **Melakukan konfigurasi ulang sandi (*password*) untuk setiap pengguna yang mungkin telah masuk ke perangkat melalui antarmuka web.**

3. **Mengaktifkan fitur *multifactor authentication* (MFA**) pada semua produk SonicWall SMA, Firewall, dan MySonicWall. Panduan untuk mengaktifkan fitur tersebut terdapat pada artikel berikut :

   a. Akun SonicWall SMA :

      https://www.sonicwall.com/support/knowledge-base/how-can-i-configure-time-based-one-time-password-totp-in-sma-100-series/180818071301745/

   b. Akun Firewall :

      https://www.sonicwall.com/support/knowledge-base/how-to-configure-two-factor-authentication-using-totp-for-https-management/190201153847934/

   c. Akun MySonicWall :

      https://www.sonicwall.com/support/knowledge-base/how-do-i-configure-2fa-for-ssl-vpn-with-ldap-and-totp/190829123329169/

4. **Mengaktifkan *Web Application Firewall* (WAF) pada SMA seri 100**. Apabila pengguna tidak dapat menggunakan WAF tersebut, untuk sementara dapat digantikan dengan mengaktifkan fitur WAF yang sudah ada pada produk untuk mengurangi kerentanan di SNWLID-2021-0001 pada perangkat SMA 100 seri 10.x. Penerapan WAF tersebut dapat mengikuti panduan yang sudah ada dalam artikel https://www.sonicwall.com/support/knowledge-base/210202202221923/.

Referensi

[1] SonicWall, "SonicWall," 4 February 2021. [Online]. Available: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001. [Accessed 8 February 2021].

[2] SingCert, "A Singapore Government Agency Website," 4 February 2021. [Online]. Available: https://www.csa.gov.sg/singcert/alerts/al-2021-005.

[3] CVE, "Common Vulnerabilities and Exposures," 2021. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-20016.

[4] S. Narang, "tenable," 4 February 2021. [Online]. Available: https://www.tenable.com/blog/cve-2021-20016-zero-day-vulnerability-in-sonicwall-secure-mobile-access-sma-exploited.

[5] SonicWall, "SonicWall," 4 February 2021. [Online]. Available: https://www.sonicwall.com/support/product-notification/urgent-patch-available-for-sma-100-series-10-x-firmware-zero-day-vulnerability-updated-feb-3-2-p-m-cst/210122173415410/&usg=alkjrhipqvkhe4fq2i7lcb_-cmice8acfg/. [Accessed 8 February 2021].

Riwayat Dokumen

Versi 1.0: 8 Februari 2021
Versi 1.1: 9 Februari 2021

Dokumen ini ditanda tangani secara elektronik oleh

ADI NUGROHO, S.ST, S.KOM
Koordinator Kelompok Tata Kelola,
Pusat Operasi Keamanan Siber Nasional
Badan Siber dan Sandi Negara