IMBAUAN KEAMANAN
KERENTANAN *ZERO-DAY* PADA PRODUK CARRIER

Senin, 13 Juni 2022

Ringkasan Eksekutif

1. Pada Kamis 2 Juni 2022, perusahaan Carrier (*Carrier Corporation*) mengeluarkan imbauan mengenai 8 kerentanan *zero-day* yang terdampak pada produk Carrier yaitu *LenelS2 Access Hardware Controller.*
2. Kerentanan ini dideskripsikan pada beberapa CVE yaitu CVE 2022-31479, CVE-2022-31480, CVE-31481, CVE-2022-31482, CVE-2022-31483, CVE-2022-31484, CVE-2022-31485, dan CVE-2022-31486 dengan sebagian besar skor CVSS di atas 7,5.
3. Mengingat dampak yang mungkin muncul dari eksploitasi kerentanan ini, diharapkan pengguna dari produk terdampak ataupun pengguna pemerintah dan publik lainnya untuk segera melakukan tindakan-tindakan mitigasi yang dijelaskan pada imbauan keamanan ini.

Pendahuluan

Carrier *Corporation* adalah perusahaan di bidang Iklim, Pengendali, dan Keamanan UTC, yang berkantor pusat di Palm Beach Gardens, Florida. Pada tanggal 2 Juni 2022, Carrier mengeluarkan imbauan mengenai 8 kerentanan *zero-day* yang terdampak pada produk Carrier yaitu *LenelS2 Access Hardware Controller*. Sam Quinn @eAyeP dan Steve Povolny @spovolny dari *Trellix Threat Labs* melaporkan kerentanan ini kepada Carrier. Adapun kerentanan yang dilaporkan oleh *Trellix Threat Labs* dideskripsikan pada beberapa CVE yaitu CVE 2022-31479, CVE-2022-31480, CVE-31481, CVE-2022-31482, CVE-2022-31483, CVE-2022-31484, CVE-2022-31485, dan CVE-2022-31486.

Nilai Kerentanan

Berdasarkan CVSS Score, 8 kerentanan *zero-day* ini memiliki sebagian besar skor CVSS di atas 7,5 dengan rincian nilai sebagai berikut:

CVE	Detail Summary	Mercury Firmware Version	CVSS Score
CVE-2022-31479	Unauthenticated command injection	<=1.291	Base 9.0, Overall 8.1
CVE-2022-31480	Unauthenticated denial-of-service	<=1.291	Base 7.5, Overall 6.7
CVE-2022-31481	Unauthenticated remote code execution	<=1.291	Base 10.0, Overall 9.0
CVE-2022-31486	Authenticated command injection	<=1.291 (no patch)	Base 8.8, Overall 8.2
CVE-2022-31482	Unauthenticated denial-of-service	<=1.265	Base 7.5, Overall 6.7
CVE-2022-31483	Authenticated arbitrary file write	<=1.265	Base 9.1, Overall 8.2
CVE-2022-31484	Unauthenticated user modification	<=1.265	Base 7.5, Overall 6.7
CVE-2022-31485	Unauthenticated information spoofing	<=1.265	Base 5.3, Overall 4.8

Gambar 1. Bagan Kerentanan Produk Carrier dari *Trellix Threat Lab* (https[:]//therecord[.]media/8-zero-day-vulnerabilities-discovered-in-popular-industrial-control-system-from-carrier)

Produk Terdampak

Produk Carrier yang terdampak oleh 8 kerentanan *zero-day* tersebut adalah HID Mercury Access Panels yang dijual oleh LenelS2 dengan nomor sebagai berikut:

- **LNL-X2210**
- **LNL-X2220**
- **LNL-X3300**
- **LNL-X4420**
- **LNL-4420**
- **S2-LP-1501**
- **S2-LP-4502**
- **S2-LP-2500**
- **S2-LP-1502**

Detail dan Dampak Kerentanan

Cybersecurity and Infrastructure Security Agency (CISA) merilis imbauan keamanan mengenai 8 kerentanan *zero-day* yang terdampak pada produk Carrier. Berdasarkan dokumen tersebut, kerentanan yang dijelaskan didalamnya adalah CVE-2022-31479, CVE-2022-31480, CVE-2022-31481, CVE-2022-31482, CVE-2022-31483 , CVE-2022-31484, CVE-2022-31485, CVE-2022-31486 dengan sebagian besar memiliki nilai CVSS di atas 7,5. Berikut merupakan rincian kerentanan *zero-day* yang terdampak pada produk Carrier:

a. *Protection Mechanism Failure* CWE-693

Penyerang yang tidak diautentikasi dapat memperbarui nama *host* dengan nama yang dibuat khusus, memungkinkan eksekusi perintah *shell* selama proses pengumpulan inti. CVE-2022-31479 telah ditetapkan untuk kerentanan ini. Skor dasar CVSS v3 9,6 telah dihitung; string vektor CVSS adalah (AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).

b. *Direct Request ('Forced Browsing')* CWE-425

Penyerang yang tidak diautentikasi dapat mengunggah file *firmware* ke perangkat target, yang pada akhirnya menyebabkan kondisi *denial-of-service*. CVE-2022-31480 telah ditetapkan untuk kerentanan ini. Skor dasar CVSS v3 7,5 telah dihitung; string vektor CVSS adalah (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

c. *Buffer Copy Without Checking Size Of Input ('Classic Buffer Overflow')* CWE-120

Penyerang yang tidak diautentikasi dapat mengirim file pembaruan yang dibuat khusus ke perangkat yang dapat menimbulkan kerentanan *buffer overflow*. CVE-2022-31481 telah ditetapkan untuk kerentanan ini. Skor dasar CVSS v3 10,0 telah dihitung; string vektor CVSS adalah (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

d. *Buffer Copy Without Checking Size Of Input ('Classic Buffer Overflow')* CWE-120

Penyerang yang tidak diautentikasi dapat mengirim permintaan HTTP yang tidak diautentikasi yang dibuat khusus ke perangkat yang menimbulkan kerentanan *buffer overflow*. CVE-2022-31482 telah ditetapkan untuk kerentanan ini. Skor dasar CVSS v3 7,5 telah dihitung; string vektor CVSS adalah (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

e. *Improper Limitation Of A Pathname To A Restricted Directory ('Path Traversal')* CWE-22

Penyerang yang diautentikasi dapat memanipulasi nama file untuk mencapai kemampuan mengunggah file yang diinginkan di mana saja di sistem file. CVE-2022-31483 telah ditetapkan untuk kerentanan ini. Skor dasar CVSS v3 9,1 telah dihitung; string vektor CVSS adalah (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).

f. *Direct Request ('Forced Browsing')* CWE-425

Penyerang yang tidak diautentikasi dapat mengirim paket jaringan yang dibuat khusus untuk menghapus pengguna dari antarmuka web. CVE-2022-31484 telah ditetapkan untuk kerentanan ini. Skor dasar CVSS v3 7,5 telah dihitung; string vektor CVSS adalah (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

g. *Direct Request ('Forced Browsing')* CWE-425

Penyerang yang tidak diautentikasi dapat mengirim paket yang dibuat khusus untuk memperbarui bagian "*notes*" di halaman beranda antarmuka web. CVE-2022-31485

telah ditetapkan untuk kerentanan ini. Skor dasar CVSS v3 5,3 telah dihitung; string vektor CVSS adalah (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).

h. *Improper Neutralization Of Special Elements Used In An Os Command ('Os Command Injection')* CWE-78

Penyerang yang diautentikasi dapat mengirim rute yang dibuat khusus ke biner tertentu yang menyebabkannya menjalankan perintah *shell*. CVE-2022-31486 telah ditetapkan untuk kerentanan ini. Skor dasar CVSS v3 8.8 telah dihitung; string vektor CVSS adalah (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).

Panduan Mitigasi

Untuk melakukan pencegahan terhadap 8 kerentanan yang terdampak pada produk milik Carrier, terdapat beberapa saran yang dapat dilakukan, yaitu:

1. Pihak Carrier merekomendasikan untuk memperbarui panel akses ke *firmware* terbaru yang dirilis melalui LenelS2 *Partner Center*. Selain itu, Carrier telah menerbitkan CARR-PSA-006-0622 untuk memberi tahu pengguna mengenai kerentanan ini, dengan tambahan memberikan petunjuk mitigasi.
2. CISA merekomendasikan pengguna mengambil langkah-langkah berikut untuk mengurangi risiko eksploitasi kerentanan ini:
   a. Meminimalkan eksposur jaringan untuk semua sistem kontrol perangkat dan/atau sistem, dan memastikan sistem tersebut tidak dapat diakses dari jaringan publik.
   b. Menempatkan jaringan sistem kontrol dan perangkat jarak jauh di belakang firewall dan memisahkan nya dari jaringan bisnis.
   c. Ketika akses jarak jauh diperlukan, maka gunakanlah metode yang aman, seperti *Virtual Private Networks* (VPNs), VPN yang digunakan harus diperbarui ke versi terbaru yang tersedia selain itu juga lakukan konfigurasi VPN dengan baik berdasarkan perangkat yang semestinya terhubung.

CISA juga mengingatkan kepada organisasi untuk melakukan analisis dampak dan penilaian risiko yang tepat sebelum menerapkan langkah-langkah pengamanan.

Riwayat Dokumen

Versi Dokumen	Tanggal Rilis
1.0	Senin, 13 Juni 2022

Ketentuan Penggunaan Dokumen

Dokumen Imbauan ini tersedia secara bebas dengan mengakses portal Website ID-SIRTII/CC. Terkait penggunaan dokumen imbauan ini, dapat digunakan oleh seluruh pihak yang menggunakan produk terdampak kerawanan yang diulas pada dokumen imbauan ini.

Referensi

[1] "8 zero-day vulnerabilities discovered in popular industrial control system from Carrier - The Record by Recorded Future." https://therecord.media/8-zero-day-vulnerabilities-discovered-in-popular-industrial-control-system-from-carrier/ (accessed Jun. 12, 2022).

[2] "Advisories & Resources | Product Security | Carrier Corporate." https://www.corporate.carrier.com/product-security/advisories-resources/ (accessed Jun. 12, 2022).

[3] "Carrier LenelS2 HID Mercury access panels | CISA." https://www.cisa.gov/uscert/ics/advisories/icsa-22-153-01 (accessed Jun. 12, 2022).

KONTAK KAMI

(021) 788 33610

bantuan70@bssn.go.id

Jl. Harsono RM No. 70, Ragunan
Pasar Minggu, Jakarta Selatan, 12550