IMBAUAN KEAMANAN KERENTANAN PADA APACHE HTTP *SERVER* (CVE 2019-17567)

Ringkasan Eksekutif

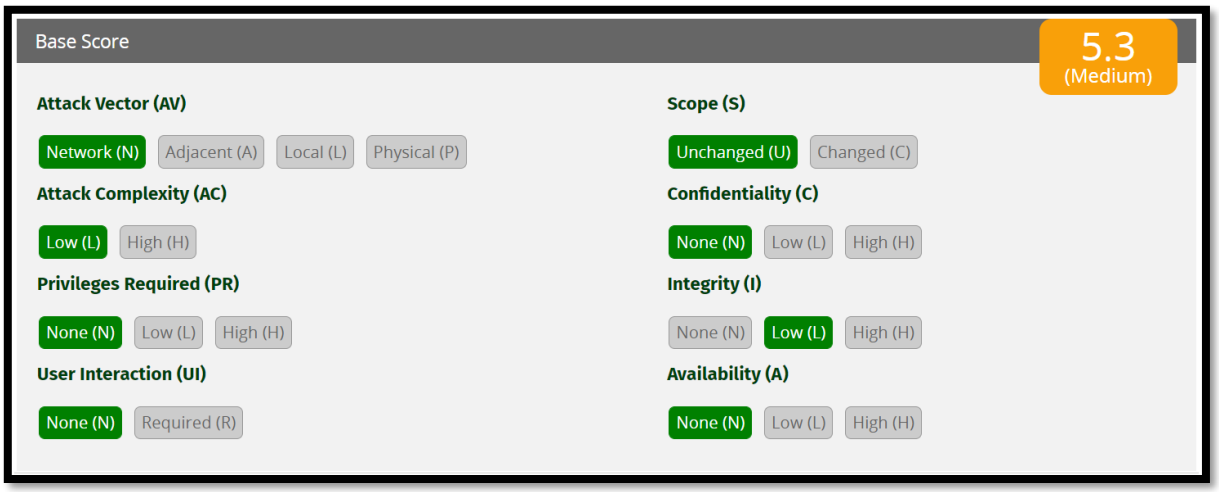
1. Pada 06 Oktober 2021, *Apache Software Foundation* merilis himbauan keamanan di httpd.apache.org. untuk kerentanan `mod_proxy_wstunnel` pada URL yang belum tentu ditingkatkan oleh server asal. Kerentanan tersebut diidentifikasi sejak 14 Oktober 2019 dan kemudian dilacak sebagai CVE 2019-17567
2. Penyebab utama kerentanan ini berkaitan dengan mod_proxy_wstunnel yang dikonfigurasikan pada URL belum tentu ditingkatkan oleh server asal, sehingga memungkinkan request berikutnya pada koneksi yang sama untuk lewat tanpa validasi HTTP, autentikasi atau otorisasi.
3. Kerentanan ini dideskripsikan pada CVE 2019-17567 sebagai kerentanan yang memiliki dampak *Medium* dengan nilai 5,3.
4. 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

Apache HTTP Server atau Server Web/WWW Apache adalah server web yang dapat dijalankan di banyak sistem operasi yang berguna untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas web/www ini menggunakan HTTP. Apache memiliki fitur-fitur seperti pesan kesalahan yang dapat dikonfigur, autentikasi berbasis basis data, dan lain-lain. Apache juga didukung oleh sejumlah user interface berbasis grafik (GUI) yang memungkinkan penanganan server menjadi mudah. Apache merupakan perangkat lunak sumber terbuka dikembangkan oleh komunitas terbuka yang terdiri dari pengembang-pengembang di bawah naungan Apache Software Foundation.

Nilai Kerentanan

Berdasarkan CVSS 3.1, kerentanan ini memiliki nilai **5.3** yang dideskripsikan dalam **CVE 2019-17567** dan dikategorikan sebagai *severity* **Medium**.



Gambar 1. *Base Score* untuk Kerentanan CVE 2019-17567
Vector String (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Produk Terdampak

Produk yang terdampak oleh CVE 2019-17567 adalah Apache HTTP Server versi 2.4.46 hingga 2.4.6.

Detail dan Dampak Kerentanan

Pada tanggal 6 Oktober 2021, Apache Software Foundation merilis himbauan keamanan di httpd.apache.org. untuk kerentanan `mod_proxy_wstunnel` pada URL yang belum tentu ditingkatkan oleh server asal. Kerentanan tersebut diidentifikasi sejak 14 Oktober 2019 dan kemudian dilacak sebagai CVE 2019-17567. CVE 2019-17567 merupakan serangan mempengaruhi fungsionalitas yang tidak diketahui dari komponen `mod_proxy_wstunnel`. Penyebab utama kerentanan ini berkaitan dengan `mod_proxy_wstunnel` yang dikonfigurasikan pada URL belum tentu ditingkatkan oleh server asal, sehingga memungkinkan request berikutnya pada koneksi yang sama untuk lewat tanpa validasi HTTP, autentikasi atau otorisasi. Pada kerentanan ini, Penyerang dapat memulai serangan dari jarak jauh tanpa dibutuhkan autentikasi untuk melakukan eksploitasi. Manipulasi dengan input yang tidak diketahui dapat menyebabkan kerentanan autentikasi yang lemah.

Berdasarkan perhitungan yang dilakukan, diperoleh informasi bahwa jaringan sebagai Attack Vector (AV), memiliki Attack Complexity (AC) yang rendah, tidak memerlukan privilege maupun user interaction. Hal ini semakin memperbesar nilai dampak karena memiliki pengertian bahwa penyerang dapat menyerang sistem tanpa membutuhkan persetujuan/interaksi dari pengguna. Selain itu, jika kerentanan ini berhasil dieksploitasi, maka akan memiliki nilai resiko yang rendah terhadap aspek integritas tanpa mempengaruhi aspek kerahasiaan dan ketersediaan. Dampak dari kerentanan ini adalah adanya request selanjutnya pada koneksi yang sama dapat melewati tanpa adanya validasi HTTP, autentikasi, dan otorisasi. Hal tersebut berdampak pada kerahasiaan, integritas, dan ketersediaan. Serangan dapat dilakukan dari jarak jauh. Tidak ada bentuk autentikasi yang diperlukan untuk eksploitasi yang berhasil.

Panduan Mitigasi

Deputi Bidang Operasi Keamanan Siber dan Sandi mengimbau agar segera melakukan langkah mitigasi lebih lanjut yang direkomendasikan untuk pihak pengelola sistem informasi. Untuk melakukan pencegahan terhadap kerentanan CVE 2019-17567, terdapat beberapa rekomendasi perbaikan yang dapat dilakukan, yaitu:

1. Melakukan pembaruan Apache HTTP Server ke versi terbaru;
2. Melakukan konfigurasi `mod_proxy_wstunnel` pada URL yang selalu di-*upgrade* oleh server asal;
3. Hanya konfigurasi yang menggunakan `mod_proxy_wstunnel` yang terpengaruh oleh kerentanan ini. Untuk meningkatkan keamanan dapat ditambahkan komentar baris "`LoadModule proxy_wstunnel_module ...`" di `/etc/httpd/conf.modules.d/00-proxy.conf` untuk konfigurasi yang tidak bergantung pada *websockets reverse proxy.*

KONTAK KAMI

(021) 788 33610

bantuan70@bssn.go.id

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

DIREKTORAT OPERASI KEAMANAN SIBER
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER