Tugas Keamanan Jaringan Komputer
Common Vulnerabilities and Exposures

Nama : Ega Aldo Firmansyah
NIM : 09011281419057
Kelas : SK8P

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

Common Vulnerabilities and Exposures
Di Website wika.co.id

PT Wijaya Karya (Persero) Tbk (WIKA) adalah salah satu perusahaan konstruksi di Indonesia. Dari hasil nasionalisasi perusahaan Belanda, Naamloze Vennotschap Technische Handel Maatschappij en Bouwbedijf Vis en Co atau NV Vis en Co, berdasarkan Peraturan Pemerintah No. 2 Tahun 1960 dan Surat Keputusan Menteri Pekerjaan Umum dan Tenaga Listrik (PUTL) No. 5 tanggal 11 Maret 1960, WIKA lahir dengan nama Perusahaan Negara Bangunan Widjaja Karja.

PT Wijaya Karya (Persero) Tbk (WIKA) memiliki sebuah website yang berdomain www.wika.co.id dari data yang didapat melalui website www.netcraft.com, diketahui website www.wika.co.id menggunakan web server Apache versi 2.4.12 dengan IP address 103.25.196.196 yang melakukan update terakhir pada 19 Mei 2017.

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT. Wijaya Karya Corporate / Direct Member IDNIC Indonesian BUMN Konstruksi Jl. D.I. Panjaitan Kav. 9 Jakarta 13340	103.25.196.196	unknown	Apache/2.4.12 FreeBSD OpenSSL/1.0.1p-freebsd	19-May-2017

Data tersebut akan digunakan untuk mencari Common Vulnerabilities and Exposures (CVE) dari website www.wika.co.id, CVE adalah kamus cyber security yang diketahui untuk kerentanan umum. Tujuan: Mengidentifikasi dan memberi nama secara terbuka kepada umum kerentanan yang berkaitan dengan versi perangkat lunak tertentu atau code bases.

Web Server Apache

Apache adalah server web yang dapat dijalankan di banyak sistem operasi (Unix, BSD, Linux, Microsoft Windows dan Novell Netware serta platform lainnya) yang berguna untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas web/www ini menggunakan HTTP.

Apache memiliki fitur-fitur canggih seperti pesan kesalahan yang dapat dikonfigurasi, autentikasi berbasis basis data dan lain-lain. Apache juga didukung oleh sejumlah antarmuka pengguna 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..

Pada Apache versi 2.4.12 terdapat hole berikut:

Apache HTTP Request Parsing Whitespace Defects (CVE-2016-8743)

Apache HTTP Server, sebelum rilis 2.4.25 (2.2.32), menerima pola pola spasi putih yang tidak biasa dari agen pengguna, termasuk CR telanjang, FF, VTAB dalam memecah jalur permintaan dan meminta baris header, serta HTAB dalam menguraikan baris permintaan Setiap CR yang ada di baris permintaan diperlakukan sebagai spasi dan tetap berada dalam daftar permintaan anggota lapangan "the_request", sementara CR yang kosong dalam nama field header permintaan akan dihormati sebagai spasi, dan CR kosong dalam nilai field header permintaan dipertahankan. masukan header array Spasi tambahan tersirat diterima di baris permintaan dan sebelum pembatas ':' dari setiap baris header permintaan.

RFC7230 Bagian 3.5 memanggil beberapa pengecualian spasi ini, dan bagian 3.2.3 menghilangkan dan mengklarifikasi peran ruang kosong tersirat di dalam daftar spesifikasi ini. Bagian 3.1.1 memerlukan tepat satu SP tunggal antara metode dan target permintaan, dan antara target permintaan dan versi HTTP, diikuti segera oleh urutan CRLF. Tak satu pun dari bidang ini mengizinkan karakter CTL apapun. Bagian 3.2.4 secara eksplisit melarang setiap spasi dari field header permintaan sebelum karakter ':', sedangkan Bagian 3.2 melarang semua karakter CTL di baris header permintaan selain karakter HTAB sebagai spasi.

Cacat ini mewakili masalah keamanan saat httpd berpartisipasi dalam rangkaian proxy atau berinteraksi dengan server aplikasi back-end, baik melalui mod_proxy atau menggunakan mekanisme CGI konvensional. Dalam setiap kasus di mana satu agen menerima karakter CTL tersebut dan tidak memperlakukannya sebagai spasi, ada kemungkinan adanya rantai proxy untuk menghasilkan dua tanggapan dari server di belakang agen proxy yang tidak berkulit putih. Dalam urutan dua permintaan, ini menghasilkan permintaan A ke proxy pertama yang ditafsirkan sebagai permintaan A + A 'oleh server backend, dan jika permintaan A dan B diajukan ke proxy pertama dalam koneksi keepalive, proxy tersebut dapat menafsirkannya. respon A 'sebagai tanggapan terhadap permintaan B, mencemari cache atau berpotensi menyajikan konten A ke agen pengguna hilir yang berbeda.

Cacat ini ditangani dengan rilis Apache HTTP Server 2.4.25 dan dikoordinasikan oleh direktif baru;

HttpProtocolOptions Ketat

yang merupakan perilaku default 2.4.25 dan yang lebih baru. Dengan mengalihkan perilaku 'Ketat' ke perilaku 'Tidak Aman', beberapa batasan mungkin santai untuk memungkinkan beberapa klien HTTP / 1.1 yang tidak valid berkomunikasi dengan server, namun ini akan mengenalkan kembali kemungkinan masalah yang dijelaskan dalam penilaian ini. Perhatikan bahwa merilekskan perilaku 'Tidak Aman' tetap tidak mengizinkan CTL mentah selain HTAB (bila diizinkan), namun mengizinkan persyaratan RFC lainnya tidak dapat diterapkan, seperti tepat dua karakter SP di baris permintaan.

Reported to security team	10th February 2016
Issue public	20th December 2016
Update Released	20th December 2016
Affects	2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1