IMBAUAN KEAMANAN KERENTANAN *REMOTE CODE EXECUTION* PADA *WINDOWS POINT-TO-POINT TUNNELING PROTOCOL* (CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081)

Senin, 17 Oktober 2022

Ringkasan Eksekutif

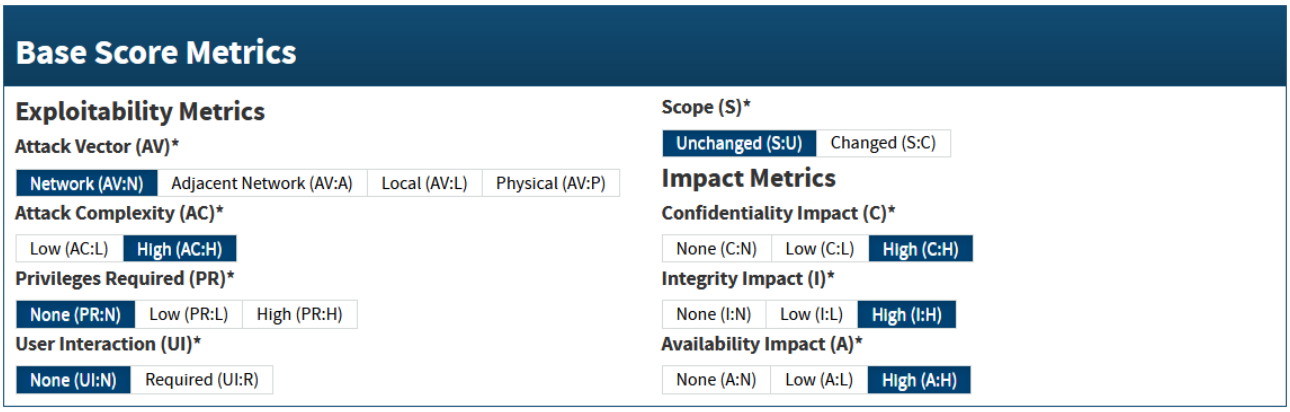
1. Pada Selasa 11 Oktober 2022, Microsoft telah merilis pembaruan untuk mengatasi beberapa kerentanan dalam perangkat lunak Microsoft, diantaranya adalah mengenai kerentanan *Remote Code Execution* (RCE) pada Windows *Point to Point* (P2P) *Tunneling Protocol*.
2. Kerentanan ini dideskripsikan pada CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081 sebagai kerentanan yang memiliki dampak *High*.
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

Microsoft pada bulan Oktober telah memperbaiki total 84 kerentanan, termasuk kelemahan *zero-day* yang dieksploitasi secara aktif. Semua kerentanan memiliki tingkat *severity high* yang dapat menyebabkan *remote code execution, privilege escalation,* atau *spoofing*. Dalam hal ini mengenai kerentanan RCE pada *Windows Point to Point Tunneling Protocol* (PPTP). Penyerang dapat mengirimkan *malicious packet* PPTP yang dibuat khusus ke server PPTP / RAS (*Remote Application Server*), kemudian dapat mengeksploitasi kerentanan ini dengan mengeksekusi kode arbitrer di dalam paket. Hal ini terjadi karena Microsoft Windows mengizinkan penyerang untuk mengirimkan paket PPTP untuk dapat mengeksekusi kode arbitrer pada sistem.

Nilai Kerentanan

Berdasarkan CVSS 3.1, kerentanan ini memiliki nilai **8.1** yang dideskripsikan dalam **CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081** dan dikategorikan sebagai *severity* ***HIGH***.



Gambar 1. *Base Score* untuk Kerentanan CVE-2022-22035, CVE-2022-24504, CVE-2022-33634, CVE-2022-38000, CVE-2022-38047, CVE-2022-41081

Vector String (CVSS:3.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

Produk Terdampak

Produk yang terdampak yaitu:

- Microsoft Windows 7 SP1 x32
- Microsoft Windows 7 SP1 x64
- Microsoft Windows Server 2012
- Microsoft Windows 8.1 x32
- Microsoft Windows 8.1 x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows RT 8.1
- Microsoft Windows 10 x32
- Microsoft Windows 10 x64
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows 10 1809 *for* x64-*based Systems*
- Microsoft Windows 10 1809 *for* 32-bit *Systems*
- Microsoft Windows 10 1809 *for* ARM64-*based Systems*
- Microsoft Windows 10 1607 *for* 32-bit *Systems*
- Microsoft Windows 10 1607 *for* x64-*based Systems*

- Microsoft Windows 10 20H2 *for* 32-bit *Systems*
- Microsoft Windows 10 20H2 *for* ARM64-*based Systems*
- Microsoft Windows 10 20H2 *for* x64-*based Systems*
- Microsoft Windows Server (*Server Core installation*) 2019
- Microsoft Windows Server (*Server Core installation*) 2016
- Microsoft Windows Server (*Server Core installation*) 2012 R2
- Microsoft Windows Server (*Server Core installation*) 2012
- Microsoft Windows Server *for* X64-*based Systems* 2008 R2 SP1
- Microsoft Windows Server *for* X64-*based Systems* (*Server Core installation*) 2008 R2 SP1
- Microsoft Windows 10 21H1 *for* 32-bit *Systems*
- Microsoft Windows 10 21H1 *for* ARM64-*based Systems*
- Microsoft Windows 10 21H1 *for* x64-*based Systems*
- Microsoft Windows Server 2022
- Microsoft Windows Server (*Server Core installation*) 2022
- Microsoft Windows 11 x64
- Microsoft Windows 11 ARM64
- Microsoft Windows 10 21H2 *for* 32-bit *Systems*
- Microsoft Windows 10 21H2 *for* ARM64-*based Systems*
- Microsoft Windows 10 21H2 *for* x64-*based Systems*
- Microsoft Windows 11 22H2 *for* ARM64-*based Systems*
- Microsoft Windows 11 22H2 *for* x64-*based Systems*

Detail dan Dampak Kerentanan

Pada Selasa 11 Oktober 2022, Microsoft telah merilis *Security Updates* untuk mengatasi beberapa kerentanan yang terdapat pada perangkat lunak berbasis sistem operasi milik Microsoft. Salah satunya adalah mengenai kerentanan RCE pada PPTP. PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari *remote client* ke server dengan membuat sebuah VPN (*Virtual Private Network*) melalui jaringan TCP/IP. PPTP pada windows diketahui dapat dimanfaatkan untuk melakukan RCE pada server RAS. Pada prosesnya, windows mengizinkan untuk mengeksekusi paket PPTP yang diterima. Hal tersebut dapat dimanfaatkan penyerang dengan membuat malicious packet PPTP untuk dikirimkan ke server RAS.

Panduan Mitigasi

Gunakan pembaruan otomatis Microsoft untuk menerapkan *patch* yang sesuai untuk sistem, atau dapat melihat *Security Update Guide* pada link berikut: https://msrc.microsoft.com/update-guide/

Riwayat Dokumen

Versi Dokumen	Tanggal Rilis
1.0	Rabu, 12 Oktober 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] *"October 2022 Security Updates"* https://msrc.microsoft.com/update-guide/releaseNote/2022-Oct (diakses Oktober 17, 2022).

[2] *"Microsoft October Patch Tuesday Fixes Actively Exploited Zero Day and 13 Critical Flaws"* https://socradar.io/microsoft-october-patch-tuesday-fixes-actively-exploited-zero-day-and-13-critical-flaws/ (diakses Oktober 17, 2022).

[3] *"Microsoft Windows Point-to-Point Tunneling Protocol code execution | CVE-2022-22035" https://www.redpacketsecurity.com/microsoft-windows-ras-point-to-point-tunneling-protocol-code-execution-cve-2022-22035/* (diakses Oktober 17, 2022)

KONTAK KAMI

(021) 788 33610

bantuan70@bssn.go.id

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