TLP:WHITE

HIMBAUAN KEAMANAN
TERKAIT *MICROSOFT BLUEKEEP VULNERABILITY*
CVE-2019-0708

Ringkasan Eksekutif

1. BlueKeep (CVE-2019-0708) merupakan kerawanan pada *Remote Desktop Protocol* (RDP) yang digunakan oleh OS Microsoft Windows meliputi **Windows 2000, Windows Vista, Windows XP, Windows 7, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R.**
2. *Remote Desktop Protocol* (RDP) merupakan salah satu fitur yang bisa ditemukan pada sistem operasi Microsoft Windows, yang memungkinkan pengguna terkoneksi ke sebuah komputer dari jarak jauh.
3. Kerentanan ini menyebabkan pengguna yang tidak sah dapat terhubung ke sistem target menggunakan RDP dengan mengirimkan permintaan yang dibuat secara khusus.
4. Kerentanan ini memiliki nilai kerentanan CVSS v3 sebesar 9,8 dan bersifat kritikal. Eksploitasi terhadap kerentanan ini memungkinkan pengambilalihan keseluruhan sistem secara *remote.*
5. Pengguna sistem operasi Windows terdampak diharapkan untuk dapat segera melakukan tindakan-tindakan mitigasi yang dijelaskan pada himbauan keamanan ini.

Kerentanan CVE-2019-0708

Remote Desktop merupakan salah satu fitur yang bisa ditemukan pada sistem operasi Microsoft Windows, yang memungkinkan pengguna terkoneksi ke sebuah komputer dari jarak jauh (*remote*). Pada sistem operasi Windows, *Remote Desktop* ini menggunakan *Remote Dektop Protocol* (RDP) yang secara *default* berjalan di TCP *port* 3389.

Remote Desktop Protocol atau sering di singkat RDP merupakan sebuah protokol jaringan yang digunakan oleh Microsoft Windows *Terminal Services* dan *Remote Desktop*. RDP dirancang berdasarkan protocol T.120 yang spesifikasinya diumumkan oleh *International Telecommunication Union* (ITU). Protokol ini juga digunakan dalam perangkat lunak konferensi jarak jauh milik Microsoft yaitu NetMeeting.

Kerentanan CVE-2019-0708 pada layanan *Remote Desktop* Windows pertama kali didaftarkan ke *Common Vulnerabilities and Exposures* pada tanggal 26 November 2018.

Kerentanan ini merupakan kerentanan *remote code execution* (RCE) pada layanan *remote desktop* Microsoft yang menyebabkan pengguna yang tidak sah dapat terhubung ke sistem target menggunakan RDP dengan mengirimkan permintaan yang dibuat secara khusus.

Remote Desktop Protocol (RDP) sendiri tidak memiliki kerentanan. Kerentanan *Remote Desktop Windows* terletak pada pra-otentikasi yang tidak memerlukan interaksi pengguna. Dengan kata lain, kerentanannya bersifat ***'wormable'***, yang berarti bahwa setiap *malware* di masa depan yang mengeksploitasi kerentanan ini dapat menyebar ke komputer lainnya dengan cara yang sama seperti *ransomware* WannaCry yang menyebar di seluruh dunia pada tahun 2017.

Sistem yang terdampak

Terdapat beberapa sistem operasi Windows yang memiliki kerentanan ini yaitu:

- Windows 2000
- Windows Vista
- Windows XP
- Windows 7
- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

Sistem operasi yang tidak memiliki kerentanan ini adalah Windows 8 dan Windows 10.

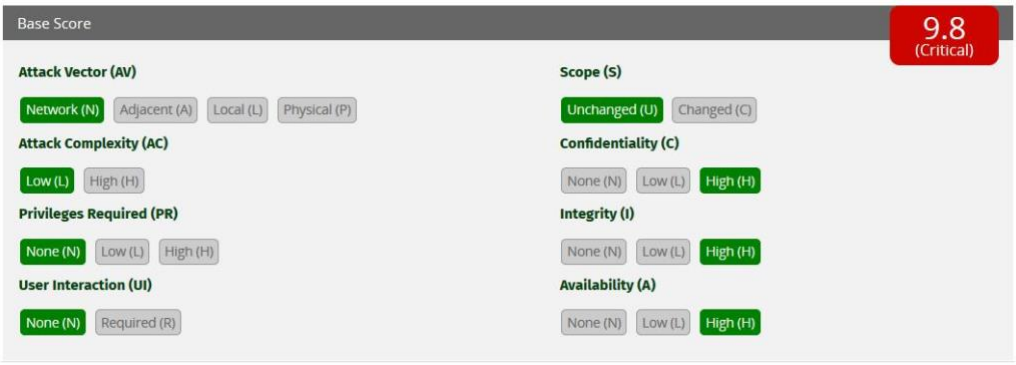
Dampak Kerentanan

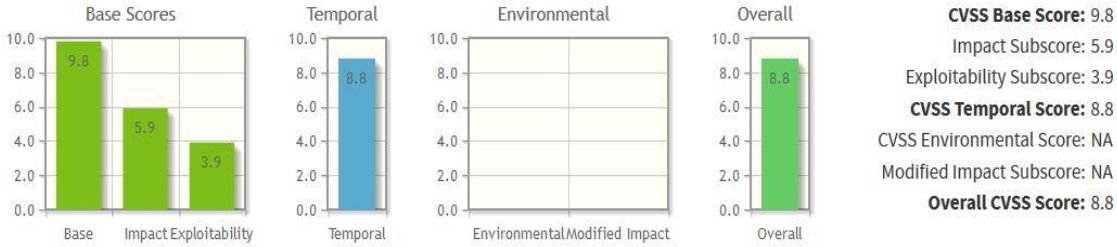
Dampak dari kerentanan CVE-2019-0708 pada layanan *Remote Desktop* Windows adalah pengguna tidak sah yang berhasil mengeksploitasi kerentanan ini dapat mengeksekusi *arbitrary code* pada sistem target. Pengguna tersebut selanjutnya dapat menginstal program, melihat, mengubah, atau menghapus data, atau membuat akun baru dengan hak pengguna penuh. Dengan kata lain, apabila kerentanan ini berhasil dieksploitasi oleh pihak yang tidak bertanggung jawab, maka berpotensi kompromi atau pengambilalihan keseluruhan sistem secara *remote*.

Nilai Kerentanan

Berdasarkan CVSS v3, kerentanan ini memiliki nilai ***base score* 9,8**, ***temporal score 8.8,*** dan **skor rata-rata sebesar 8.8** sehingga kerentanan ini termasuk kategori tinggi.

(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C)





Panduan Mitigasi Kerentanan

Berikut merupakan langkah-langkah mitigasi yang dapat dilakukan untuk menghindari dampak dari kerentanan *remote desktop* Windows:

1. **Menginstal pembaruan sistem operasi Windows**

   Pada tanggal 14 Mei 2019, Microsoft telah merilis perbaikan untuk kerentanan pada layanan *remote desktop* (CVE-2019-0708). Pembaruan ini memperbaiki bagaimana layanan *remote desktop* menangani sebuah permintaan koneksi. Pengguna sistem operasi Windows yang rentan terhadap kerentanan ini diharapkan segera melakukan pembaruan sistem operasi Windows yang digunakan. Untuk informasi lebih lanjut mengenai pembaruan dapat dilihat pada tautan https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708.

   - Untuk pengguna versi Windows yang mendukung dan memiliki pembaruan otomatis yaitu **Windows 7, Windows Server 2008 R2, dan Windows Server 2008** dapat **mengaktifkan pembaruan otomatis**.
   - Sedangkan pengguna versi Windows yang tidak didukung yaitu **Windows 2003 dan Windows XP** dapat **melakukan pembaruan dengan mengunduh *patch* yang terdapat pada portal Microsoft.**

2. Untuk sistem operasi **Windows yang sudah tidak didukung *patch* terbaru**, langkah-langkah mitigasi berikut dapat digunakan untuk membantu melindungi terhadap kerentanan BlueKeep:

   a. **Menonaktifkan layanan *remote desktop* apabila tidak diperlukan**

      Jika pengguna jarang menggunakan atau tidak lagi membutuhkan layanan ini, disarankan untuk menonaktifkannya sehingga dapat terhindari dari risiko kerentanan yang terdapat pada layanan ini.

   b. **Mengaktifkan *Network Level Authentication* (NLA) pada sistem yang menjalankan Windows 7, Windows Server 2008, dan Windows Server 2008 R2 yang didukung**.

      Pengguna dapat mengaktifkan Network Level Authentication untuk memblokir penyerang yang tidak terautentikasi dari upaya mengeksploitasi kerentanan ini. Dengan menerapkan NLA, penyerang harus mengautentikasi dirinya ke layanan Remote Desktop menggunakan akun yang valid pada sistem target sebelum penyerang bisa mengeksploitasi kerentanan.

   c. **Menutup TCP *port* 3389 di perimeter *firewall***

      TCP port 3389 digunakan untuk memulai koneksi dengan komponen yang terpengaruh. Menutup port ini dapat membantu melindungi sistem yang ada di balik firewall dari upaya

eksploitasi kerentanan CVE-2019-0708. Hal ini dapat membantu melindungi jaringan dari serangan yang berasal dari luar perimeter. Hal yang perlu diingat adalah menutup port yang terkena dampak kerentanan dapat mencegah serangan berbasis internet, namun sistem masih rentan terhadap serangan yang berasal dari dalam perimeter.

d. **Melakukan pemindaian untuk mengetahui apakah komputer atau *server* yang dikelola memiliki kerentanan CVE-2019-0708.**

   Pemindaian bertujuan untuk memastikan apakah komputer atau *server* yang menjalankan sistem operasi Windows memiliki kerentanan ini. Pemindaian juga perlu dilakukan setelah dilakukan *security patch* atau pembaruan terhadap sistem operasi Windows yang digunakan dengan tujuan untuk memastikan bahwa kerentanan CVE-2019-0708 sudah berhasil ditutup. **Panduan teknis untuk melakukan pemindaian terlampir.**

Referensi

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708
[2] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?calculator&version=3&vector=(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C)
[3] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
[4] https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/
[5] https://www.bleepingcomputer.com/news/security/bluekeep-remote-desktop-exploits-are-coming-patch-now/
[6] https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-stands-for-really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708/
[7] https://searchenterprisedesktop.techtarget.com/definition/remote-desktop
[8] https://www.first.org/cvss/calculator/3.0
[9] https://github.com/zerosum0x0/CVE-2019-0708

Lampiran

Panduan Pemindaian terhadap Kerentanan CVE-2019-0708

Pemindaian terhadap kerentanan CVE-2019-0708 berikut menggunakan *tools* yang dapat diperoleh dari alamat https://github.com/zerosum0x0/CVE-2019-0708.

Pelengkapan yang dibutuhkan

Berikut merupakan perlengkapan yang dibutuhkan untuk melakukan pemindaian terhadap kerentanan CVE-2019-0708:

No	Perlengkapan	Keterangan
1	1 unit Komputer atau *virtual machine* yang menjalankan sistem operasi Linux	Disarankan menggunakan sistem operasi Ubuntu. Komputer ini akan digunakan untuk melakukan pemindaian
2	*Tools* pemindaian	Diperoleh dari https://github.com/zerosum0x0/CVE-2019-0708

Langkah-Langkah Pemindaian

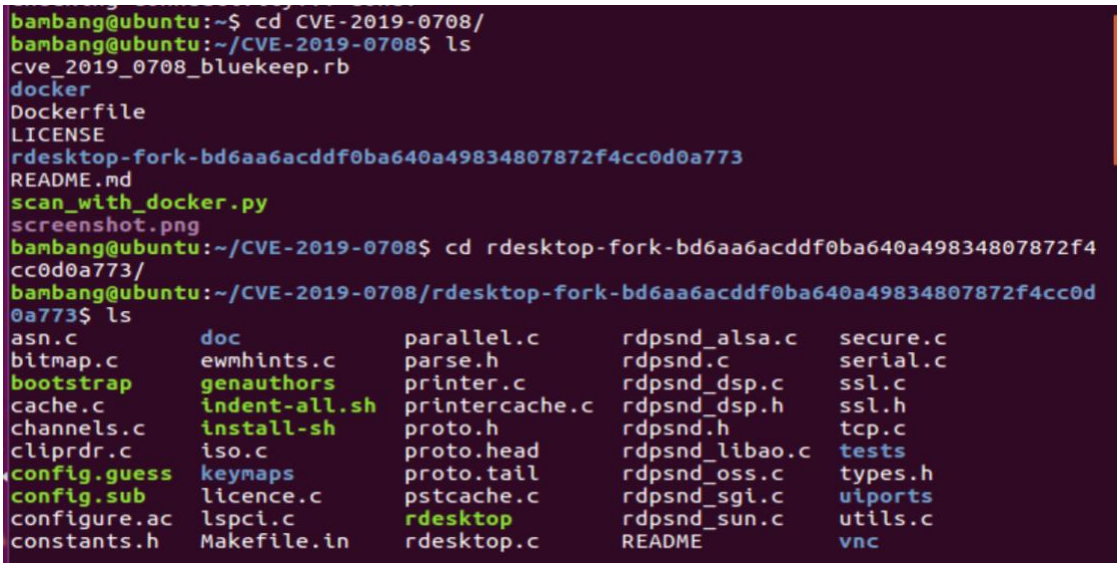
1. Buka aplikasi Terminal pada komputer Linux yang digunakan untuk melakukan pemindaian.

2. Pada aplikasi terminal, jalankan perintah berikut ini untuk mengunduh *tools* pemindaian

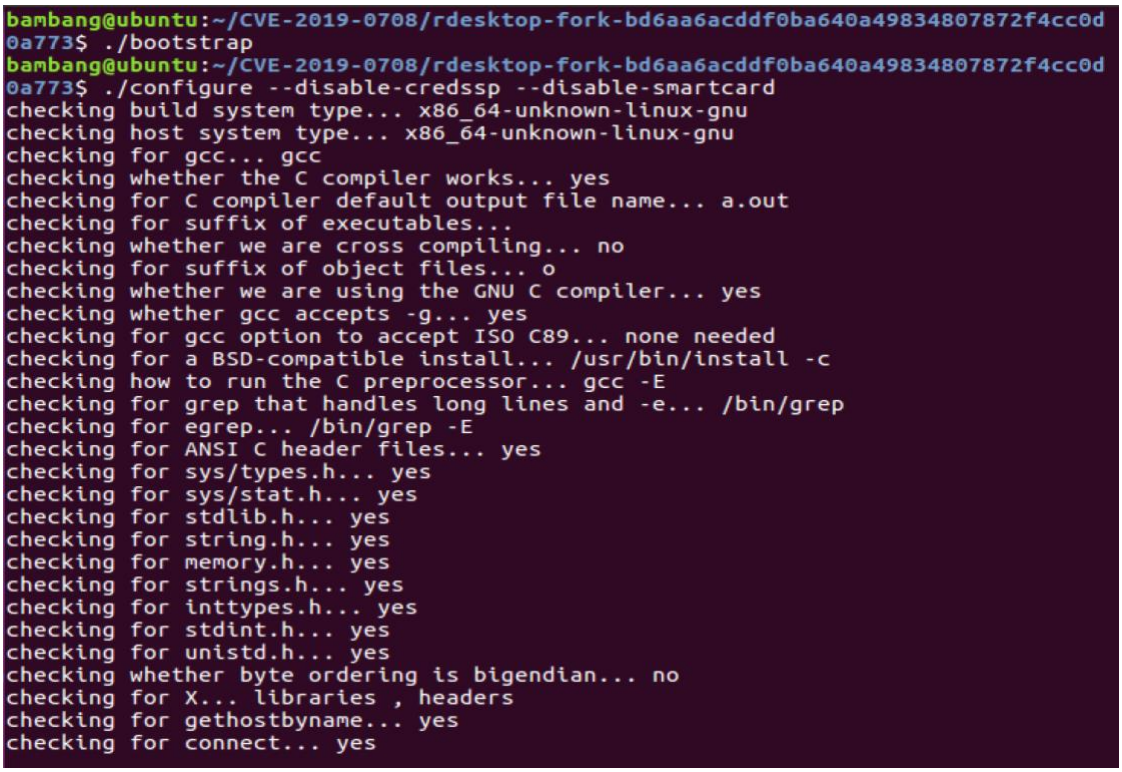
```
bambang@ubuntu:~$ git clone https://github.com/zerosum0x0/CVE-2019-0708.git
Cloning into 'CVE-2019-0708'...
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 330 (delta 8), reused 9 (delta 3), pack-reused 313
Receiving objects: 100% (330/330), 1.02 MiB | 660.00 KiB/s, done.
Resolving deltas: 100% (120/120), done.
Checking connectivity... done.
```

3. Jalankan perintah berikut untuk masuk ke dalam direktori yang menyimpan *tools* pemindaian dengan perintah

```
cd CVE-2019-0708/rdesktop-fork-bd6aa6acddf0ba640a49834807872f4cc0d0a773/
```



4. Melakukan konfigurasi *tools* pemindaian sebagai berikut.



5. Lakukan pemindaian dengan cara menjalankan perintah berikut

```
./rdesktop <alamat IP komputer atau server yang dipindai>
```

Contoh:

Jalankan perintah di bawah ini untuk melakukan pemindaian terhadap komputer dengan alamat IP **192.168.0.114.**

```
./rdesktop 192.168.211.126:3389
```

6. *Tools* akan menampilkan hasil pemindaian yang dilakukan. Contoh hasil pemindaian terhadap komputer yang memiliki kerentanan CVE-2019-0708 adalah sebagai berikut: