Vicko Bhayyu / 09011181520036

Sistem Komputer 2015 / Universitas Sriwijaya

**Microsoft Edge Scripting Engine Memory Corruption**

## Diambil dari CVE-2018-0769

Kasus :

Vulnerability terletak pada Scripting Engine Microsoft Edge yang mengurus objek memori. Vulnerability ini dapat menyebabkan memori korup, jika penyerang dapat mengeksekusi arbitrary code (Remote Code Execution). Penyerang juga dapat mendapatkan akses user administrator jika current user yang sedang login mempunyai hak user administrative. Penyerang dapat menginstall program, merubah atau menghapus data, serta dapat membuat akun baru dengan akses full.

Vulnerability ini teridentifikasi pada produk Microsoft Edge dengan platform :

* Windows 10 Version 1703 32bit
* Windows 10 Version 1709 32bit
* Windows 10 Version 1709 64bit
* Windows 10 32bit
* Windows 10 64bit
* Windows 10 Version 1709 64bit
* Windows 10 Version 1511 64bit
* Windows 10 Version 1607 32bit
* Windows 10 Version 1607 64bit
* Windows 10 Version 1511 32bit
* Windows Server 2016
* ChakraCore

Skenario Penyerangan :

Penyerang akan melakukan serangan web-based, dengan membuat website yang didesign secara khusus untuk memanfaatkan vulnerability scripting engine ini dan meyakinkan user untuk melihat, agar penyerang dapat memanfaatkan vulnerability ini.

Skenario Penanggulangan :

Vulnerability dengan tingkat keparahan Critical ini telah ditanggulangi oleh Microsoft dengan memberikan System Update pada Windows 10 (KB4056892) dan pada ChakraCore dengan mengupdate versinya menjadi v1.7.6

Pada website exploitdb juga tercantum data exploit yang membuat vulnerability pada chakracore.

Referensi :

## (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0769>)

* (<https://www.exploit-db.com/exploits/43710/>)
* (<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0769>)