

# MICROSOFT EDGE

Microsoft Edge (codename "Spartan") adalah browser web yang dikembangkan oleh Microsoft dan disertakan dalam Windows 10, Windows 10 Mobile dan Xbox One, menggantikan Internet Explorer sebagai browser web standar pada semua kelas perangkat. Menurut Microsoft, ini dirancang untuk menjadi browser web ringan dengan mesin tata letak yang dibangun di sekitar standar web. Ini memiliki fitur baru, termasuk integrasi dengan Cortana, alat anotasi, dan mode bacaan.

Edge tidak mendukung ActiveX atau Browser Helper Objects dari Internet Explorer. Dukungan ekstensi browser dikembangkan dan ditambahkan dalam pratinjau yang dibuat pada bulan Maret 2016, dan diluncurkan dengan Pembaruan Ulang Windows 10 pada tanggal 2 Agustus 2016. Ekstensi Microsoft Edge didistribusikan melalui Microsoft Store.

## FITUR

- Microsoft Edge adalah browser web default pada konsol Windows 10, Windows 10 Mobile, dan Xbox One, menggantikan Internet Explorer 11 dan Internet Explorer Mobile. Microsoft awalnya mengumumkan bahwa Edge akan mendukung mesin tata letak Trident (MSHTML) warisan untuk kompatibilitas mundur, namun kemudian mengatakan bahwa, karena "umpan balik yang kuat", Edge akan menggunakan mesin baru, sementara Internet Explorer akan terus menyediakan mesin lawas.
- Favorites, daftar bacaan, riwayat penjelajahan dan unduhan dilihat di Hub, sidebar menyediakan fungsionalitas yang mirip dengan pengelola Unduhan Internet Explorer dan Favorites Center.
- Browser mencakup Adobe Flash Player dan PDF reader yang terintegrasi. Ini juga mendukung asm.js.
- Edge tidak mendukung teknologi lawas seperti ActiveX dan Browser Helper Objects, dan malah menggunakan sistem ekstensi. Internet Explorer 11 akan tetap tersedia bersama Edge pada Windows 10 untuk kompatibilitas; itu akan tetap hampir identik dengan versi Windows 8.1 dan tidak menggunakan mesin Edge seperti yang telah diumumkan sebelumnya.

## RANKING

### - CVSS Scores & Vulnerability Types

CVSS Score	<b>5.8</b>
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	<a href="#">74</a>

## **HOW TO ATTACK**

Peningkatan kerentanan hak istimewa ada saat Microsoft Edge tidak menerapkan kebijakan lintas-domain dengan benar, yang memungkinkan penyerang mengakses informasi dari satu domain dan menyuntikkannya ke domain lain.

Dalam skenario serangan berbasis web, penyerang bisa menjadi tuan rumah sebuah situs web yang digunakan untuk mencoba memanfaatkan kerentanan tersebut. Selain itu, situs web dan situs web yang dikompromikan yang menerima atau meng-host konten yang disediakan pengguna dapat berisi konten khusus yang dapat memanfaatkan kerentanan tersebut. Namun, dalam semua kasus, penyerang tidak memiliki cara untuk memaksa pengguna melihat konten yang dikuasai penyerang. Sebagai gantinya, penyerang harus meyakinkan pengguna untuk mengambil tindakan. Misalnya, penyerang bisa mengelabui pengguna agar mengklik link yang membawa mereka ke situs penyerang. Penyerang yang berhasil mengeksploitasi kerentanan ini dapat meningkatkan hak istimewa di versi Microsoft Edge yang terpengaruh.

Pembaruan keamanan mengatasi kerentanan dengan membantu memastikan bahwa kebijakan lintas domain diterapkan dengan benar di Microsoft Edge.

## **ANALISIS HOLE**

Hole ini dapat menyebabkan Beberapa kerentanan di Microsoft Edge. Pengguna jarak jauh dapat menyebabkan kode sewenang-wenang dieksekusi pada sistem pengguna target. Pengguna jarak jauh dapat memotong kontrol keamanan lintas domain pada sistem target. Pengguna jarak jauh dapat memperoleh informasi yang berpotensi sensitif pada sistem target.