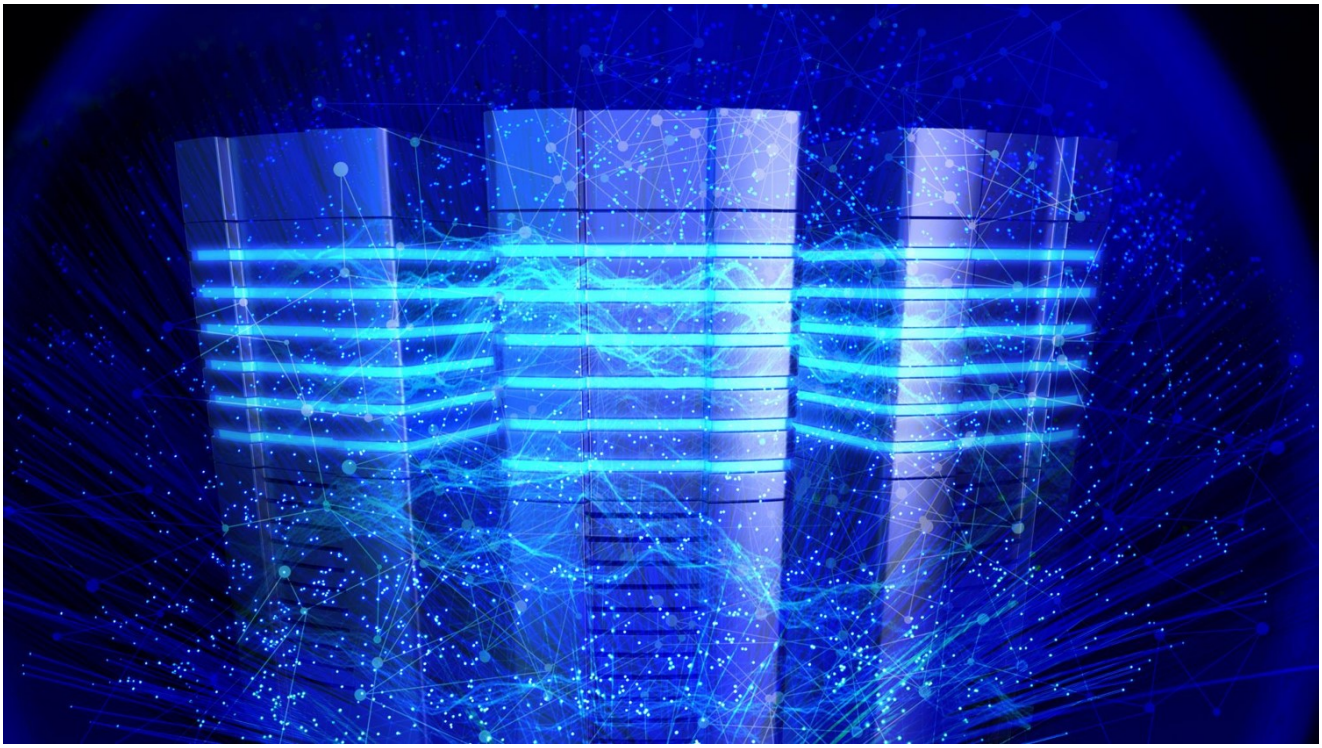
Hypervisor Introspection Thwarts Web Memory Corruption Attack in the Wild

businessinsights.bitdefender.com/hypervisor-introspection-thwarts-web-memory-corruption-attack-in-the-wild



By **Michael Rosen** / Feb 10, 2020

- New remote memory corruption vulnerability in Internet Explorer browsers allows for full takeover of infected systems
- Bitdefender has confirmed exploitation in the wild of CVE-2020-0674 with analysis of 2 distinct executable payloads
- Hypervisor Introspection delivers true zero-day protection by preventing all common memory exploit techniques

On January 17, Microsoft announced Security Advisory ADV200001, describing a zero-day remote code execution in Internet Explorer that has been actively exploited in the wild. This announcement continues the parade of devastating memory-space exploits including EternalBlue and BlueKeep.

Security Advisory ADV200001 | Microsoft Guidance on Scripting Engine Memory Corruption Vulnerability

CVE-2020-0674 is a recently discovered browser vulnerability in the Microsoft scripting engine that allows for remote code execution (RCE) on Internet Explorer browsers from malicious JavaScript (.js) files. The exploit carries Microsoft's highest severity rating of

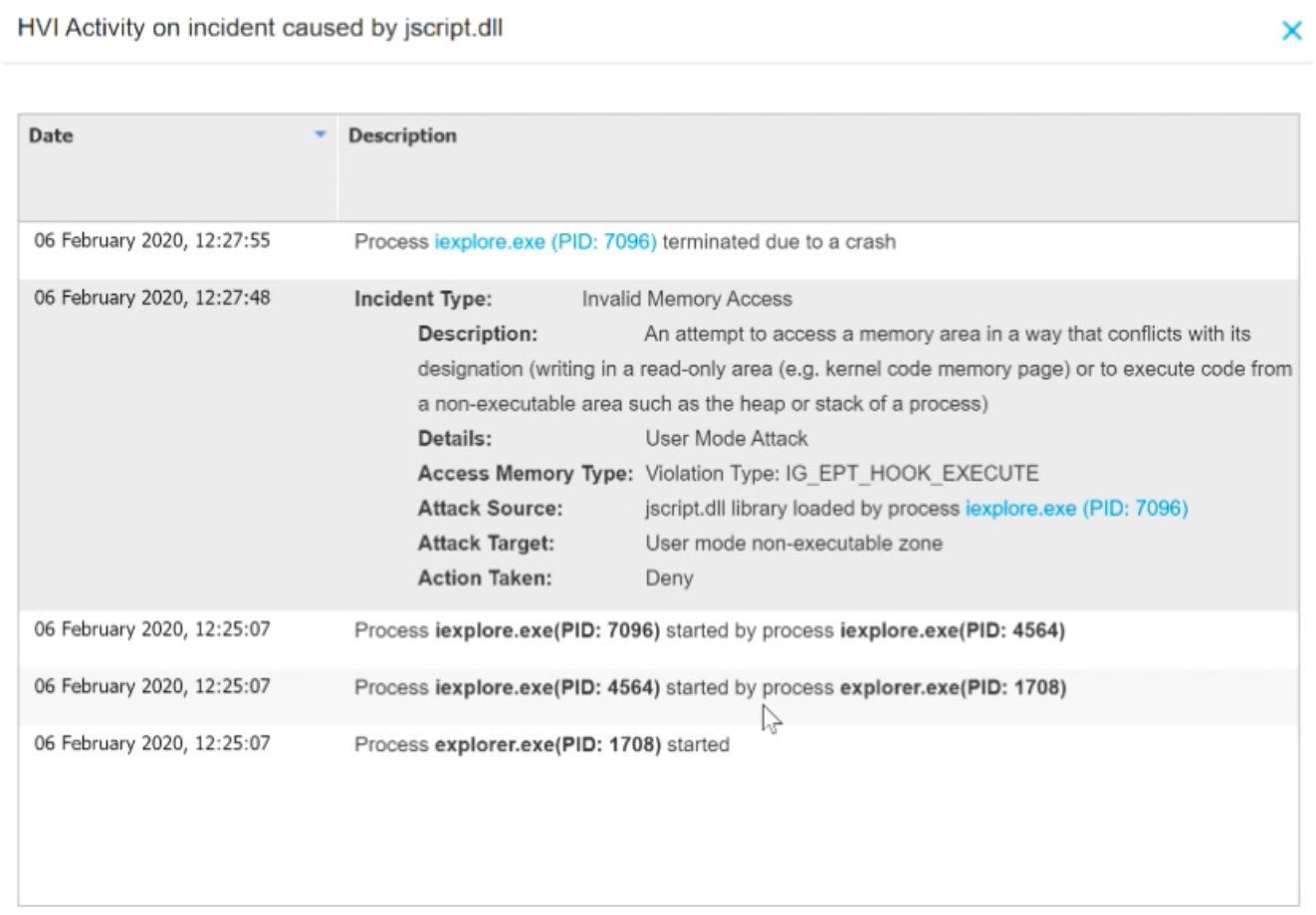
Critical and it affects Internet Explorer versions 9, 10, and 11.

Microsoft, DHS Warn of Zero-Day Attack Targeting IE Users

Bitdefender has confirmed that this critical vulnerability is being actively exploited in the wild. Security researchers in Bitdefender Labs have obtained and analyzed multiple samples to explore its tactics, techniques, and procedures. We have independently verified that 2 distinct executable payloads are unleashed by the exploit and currently in circulation:

- 785a48daa5d6d3d1abbc91eeecf9943a0fa402084cea4e66e6c2e72c76107b86
- 53f213309adce8b2bab567a16fd1bb71cc1199c65ac384345d0877ad1e9798a2

Below are Bitdefender's analysis and key findings concerning the exploitation of CVE-2020-0674 in the wild. We also demonstrate the successful detection and defeat of this dangerous exploit in virtual datacenter systems protected by Bitdefender Hypervisor Introspection (HVI)—including standard desktops, servers, and VDI desktops. HVI prevents this type of exploit, closing the gap between the time exploit code is used in the wild and the time the systems are patched.



Hypervisor Introspection intercepts and denies the attempt to access and overwrite protected memory areas.

Instead of scanning millions of malware samples, Bitdefender Hypervisor Introspection detects all known memory attack techniques—few in number and only visible at the hypervisor level—identifying advanced and zero-day attacks as easily as any known exploit, preventing the malicious behavior from executing. HVI requires no signature updates, since the common attack techniques remain relatively constant, even as the tools and procedures change with each specific attack. Bitdefender Labs maintains constant vigilance, keeping pace with new techniques and adding them to HVI's detection stack.

Bitdefender Hypervisor Introspection | Stop Advanced Targeted Attacks and Prevent Breaches

Key Findings

1. Malicious URLs from phishing links contain multiple JavaScripts, each operating on a different version of Windows to exploit CVE-2020-0674

1. When the RCE memory-space exploit is successful, the scripts download and run two distinct executable files in memory with the privileges of the logged-in user

1. The attack attempts to access a protected memory area, to write data to read-only memory, and to execute arbitrary code from a non-executable area such the heap stack or process stack

Watch Video At:

https://youtu.be/HQvWgu1H8rY

Impact of Virtualization Security on Your VDI Environment White Paper

Conclusions

Hypervisor Introspection is essential in the virtual datacenter, where built-in protection against new memory exploits and other advanced attacks using well-known exploit techniques cannot come at the expense of VM efficiency, density, or performance. Don’t rely on vendor software patches to keep you safe, as the attackers will always be one step ahead. Instead, proactively take away their operating space with HVI and set your defenses on the high ground of memory space. Bitdefender has demonstrated proactive prevention of memory vulnerabilities and exploits time and again—from EternalBlue to BlueKeep and more—proving that proactive defense with denial is always better than reactive detection.

For further information on Bitdefender Hypervisor Introspection, please download our datasheet or contact us here.