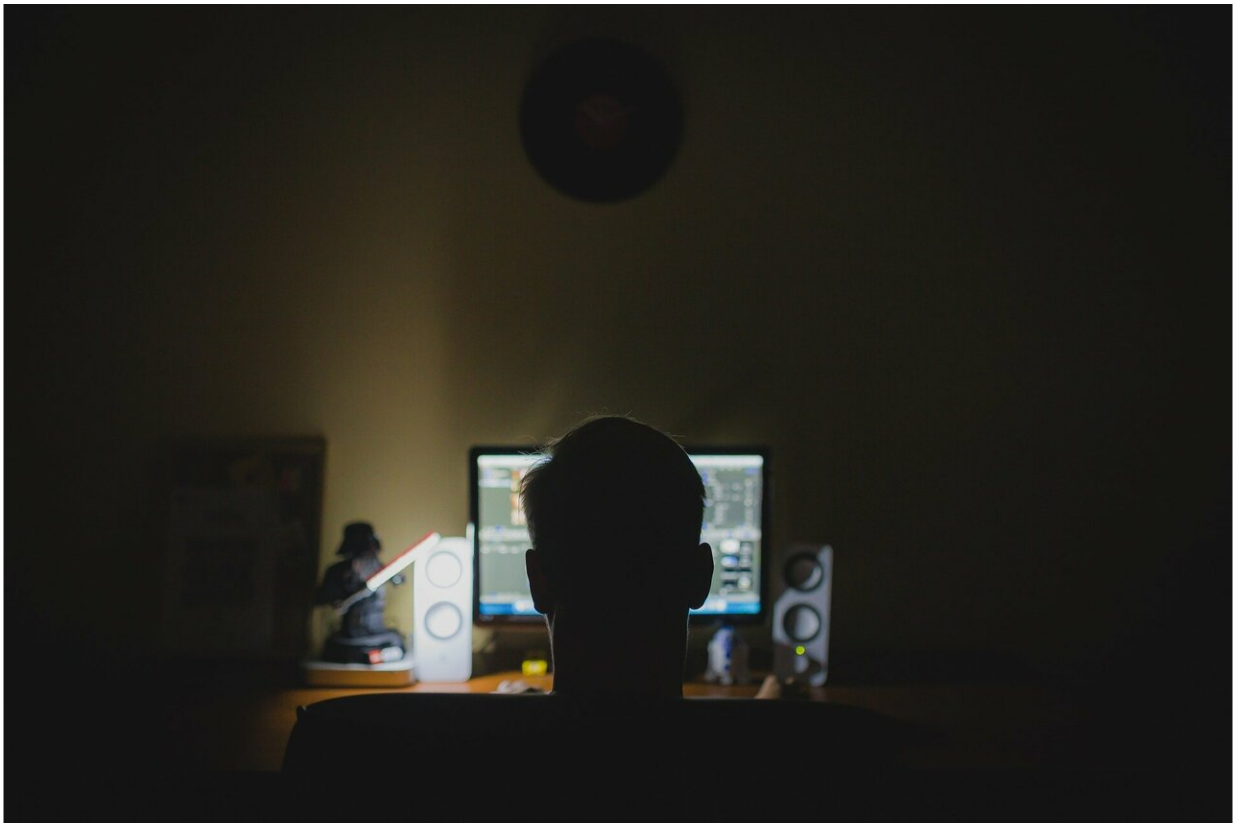
TechXplore

Microsoft patches Internet Explorer memory corruption vulnerability

March 11 2021, by Sarah Katz



Credit: CC0 Public Domain

On March 9, 2021, Microsoft patched a zero-day security vulnerability related to memory corruption in its browser, Internet Explorer.

Labeled CVE-2021-26411, this vulnerability allowed an attacker to deceive a user into visiting a uniquely crafted, malicious website hosted on Internet Explorer. Additionally, an attacker could compromise existing websites by posting malicious advertisements on webpages allowing user-hosted content. While the attacker would first have to use email or instant message to convince the user to engage with these advertisements and websites in order to compromise the victim, malicious actors from across potentially the entire Internet could take advantage of this exploit.

Because the vulnerability existed on the network stack, this CVE qualified as remotely executable. Moreover, the attacker did not require any special escalated privileges to exploit the vulnerability. Once an attack proved successful, an attacker could potentially modify any accessed files and other user information, thus placing the user's content integrity at significant risk.

Perhaps most interestingly, the hackers in this case spent weeks building trust specifically with security researches as their target. Since discovery, researchers have traced the attack back to North Korea. The attackers developed a working connection by contacting researchers via an original research blog and created Twitter personas to request collaboration on a project. The fake social media profiles would then prompt the researchers to visit a webpage. From there, even a fully patched Windows 10 machine would end up installing a malicious service and in-memory backdoor to communicate with an attacker-controlled server.

Google has attributed the attack to the North Korean government, specifically a threat group called Zinc, linked to the better-known Lazarus. Related to the devastating 2017 ransomware campaign WannaCry, Lazarus has allegedly ranked in $2 billion for North Korea's weapons of mass destruction program.

In addition to Internet Explorer, this vulnerability also impacted Edge, Microsoft's more secure browser. Furthermore, researchers eventually found that the attackers supplemented their watering-hole attack using malicious websites with a fraudulent Visual Studio Project evidently containing source code for a proof-of-concept exploit. This alleged project actually housed custom malware that contacted the hackers' control server.

As of now, the vendor has released an official fix and upgrade for this vulnerability. Those Microsoft users who desire immediate updates can visit Start > Settings > Updates & Security > Windows Update on their system.

More information: "Internet Explorer Memory Corruption Vulnerability." Security Update Guide – Microsoft Security Response Center, Microsoft, 9 Mar. 2021, msrc.microsoft.com/update-guid … ility/CVE-2021-26411

Goodin, D. "Critical 0-Day That Targeted Security Researchers Gets a Patch from Microsoft." Ars Technica, Ars Technica, 9 Mar. 2021, arstechnica.com/gadgets/2021/0 … -target-researchers/

Citation: Microsoft patches Internet Explorer memory corruption vulnerability (2021, March 11) retrieved 5 May 2024 from https://techxplore.com/news/2021-03-microsoft-patches-internet-explorer-memory.html