Microsoft Critical Vulnerability CVE-2020-1380

Vulnerability Bulletins | TLP: WHITE | Alert Id : 7477046a | Aug 13, 2020, 03:27 PM

On August 11, 2020, Microsoft rolled out Patch Tuesday updates for security flaws in its Windows operating systems and other products. Many of the discovered vulnerabilities are critical as they are being exploited by threat actors or malware targeting affected systems. At the forefront is critical vulnerability CVE-2020-1380, which is a remote code-execution bug that exposes a flaw in Internet Explorer that could allow an attacker to execute arbitrary code in the context of the current user.

CVE-2020-1380 is being actively exploited in the wild and Health-ISAC recommends members apply these patches as soon as possible in their environments.

Successful exploitation of the vulnerability will allow a threat actor to gain the same user rights as the current user. If an attacker successfully exploited the vulnerability while the current user was logged on with administrative user rights, effectively, they would be able to take control of the system. Upon gaining access to the affected system, attackers will be able to install programs, commit arbitrary acts on data, or create new accounts with full user rights.

The vulnerability allows for exploitation through a host of formulated attacks. Threat actors can conduct web-based attacks by convincing the user to view a specially crafted website that is designed to exploit the vulnerability within Internet Explorer. An attacker could also embed an ActiveX control marked “safe for initialization” in an application or Microsoft Office document that hosts the IE rendering engine. In other attacks, threat actors can take advantage of compromised websites such as ones that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.

Security researchers have confirmed critical vulnerability CVE-2020-1380 is being actively exploited in the wild. Below are the affected systems that are susceptible to exploitation if not properly patched.

- Microsoft Windows
- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge (Chromium-based) in IE Mode
- Microsoft ChakraCore
- Internet Explorer
- Microsoft Scripting Engine
- SQL Server
- Microsoft JET Database Engine
- .NET Framework
- ASP .NET Core
- Microsoft Office
- Microsoft Office Services and Web Apps
- Microsoft Windows Codecs Library
- Microsoft Dynamics

Event date: August 13, 2020

Recommendations:

Since CVE-2020-1380 is being actively exploited in the wild, Health-ISAC recommends members apply these patches as soon as possible in their environments. Health-ISAC recommends the following actions be taken:

- Apply appropriate patches or appropriate mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing
- Run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack
- Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources
- Apply the Principle of Least Privilege to all systems and services

Sources:

Microsoft Security Update Guide: CVE-2020-1380 Scripting Engine Memory Corruption Vulnerability
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1380

Krebs on Security
https://krebsonsecurity.com/2020/08/microsoft-patch-tuesday-august-2020-edition/

Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Publication
https://healthsectorcouncil.org/hhs-and-hscc-release-voluntary-cybersecurity-practices-for-the-health-industry/

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Get access to the new H-ISAC Intelligence Portal: Enhance your personalized information-sharing community with improved threat visibility, new noti cations, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments: Please email us at contact@h-isac.org.