Critical Patches Issued for Microsoft Products, August 11, 2020

Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

There are no reports of these vulnerabilities being exploited in the wild.

August 12 – UPDATED THREAT INTELLIGENCE:
Critical vulnerability CVE-2020-1380 included in this roll up addresses a vulnerability in the way that the scripting engine handles objects in memory in Internet Explorer. Successful exploitation of this vulnerability could allow an attacker to gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. Microsoft has confirmed CVE-2020-1380 is being actively exploited in the wild.

September 14 – UPDATED THREAT INTELLIGENCE:
Critical vulnerability CVE-2020-1472 remediated in this roll up addresses a vulnerability in Microsoft’s Netlogon authentication process which enables authentication bypass within a domain environment. Secura has released a publicly available Proof-Of-Concept for this vulnerability.

SYSTEMS AFFECTED:
- 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 and Microsoft Office Services and Web Apps
- Microsoft Windows Codecs Library
- Microsoft Dynamics

**RISK:**

**Government:**
- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**
- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users:** **Low**

**TECHNICAL SUMMARY:**
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution.

A full list of all vulnerabilities can be found at the link below:

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

**RECOMMENDATIONS:**
We recommend 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.

**REFERENCES:**
Microsoft:

August 12 – UPDATED REFERENCE:
US-CERT:

**September 14 – UPDATED REFERENCE:**
Github:
https://github.com/SecuraBV/CVE-2020-1472

Secura:
https://www.secura.com/blog/zero-logon

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.