TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2018-142

DATE(S) ISSUED: 12/19/2018

SUBJECT: A Vulnerability in Microsoft Internet Explorer Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Microsoft Internet Explorer, which could allow for arbitrary code execution. Microsoft Internet Explorer is a web browser available for Microsoft Windows. Successful exploitation of this vulnerability could allow for arbitrary code execution. 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.

THREAT INTELLIGENCE: There are reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- Internet Explorer 8 for Windows Embedded Standard 2009 XP, POSReady 2009
- Internet Explorer 9 for Windows Server 2008
- Internet Explorer 10 for Windows Server 2012
- Internet Explorer 11 for Windows 7, 8.1, RT 8.1, 10
- Internet Explorer 11 for Windows Server 2008 R2, 2012 R2, 2016, 2019

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:
A vulnerability has been discovered in Microsoft Internet Explorer, which could allow for arbitrary code execution. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website, for example, by sending an email. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.

Successful exploitation of this vulnerability could allow for arbitrary code execution. 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:
- Install updates provided by Microsoft, when available, after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Microsoft:
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8653
https://blogs.technet.microsoft.com/msrc/2018/12/19/december-2018-security-update-release-2/

24×7 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