From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>

Sent: Saturday, January 18, 2020 1:05 AM

To: Thomas Duffy <Thomas.Duffy@cisecurity.org>

Subject: MS-ISAC CYBERSECURITY ADVISORY - A Vulnerability in Microsoft Internet Explorer Could Allow for Arbitrary Code Execution - TLP: WHITE

TLP: WHITE

MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:

2020-010

DATE(S) ISSUED:

01/18/2020

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 limited CVE-2020-0674 exploitation in the wild.

SYSTEMS AFFECTED:

- 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, 2008 R2, 2012, 2012 R2, 2016, 2019

RISK:

Government:

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

Businesses:

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

Home users: Medium

TECHNICAL SUMMARY:

A vulnerability has been discovered in Microsoft Internet Explorer, which could allow for arbitrary code execution. The vulnerability occurs due to a memory corruption issue in the Internet Explorer Scripting

Engine. In a web-based attack scenario, an attacker could convince a user to view a specially crafted website via Internet Explorer. The workaround 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:

- Apply the mitigating workarounds provided by Microsoft, until patches are available, 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:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200001

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0674

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

My name is Mary Till and I am the Town Moderator in Derry. I rise in support of HB 1390. I have been working for over five years now to get the attention of this body to take seriously the vulnerability of our Accu-vote vote counting system to deliberate vote manipulation. The fact that I am here again today is evidence of my complete failure in this regard. But I cannot give up because democracy is a sham if the votes of the people are not protected.

Today I rise for the purpose of introducing into evidence a Cybersecurity Alert, that was issued last week
by the Multi-State Information Sharing Analysis Center, concerning a vulnerability in Microsoft Internet Explorer that could allow for arbitrary code execution. But Internet Explorer is not the only web browser impacted. Similar alerts have been issued with respect to Microsoft Word, Excel, Office, and Office 365; for Google Chrome and Android, Apple operating systems (MacOS), Safari, and IPAD, Firefox, Adobe Reader, and Oracle, to name a few. If you will not believe me with respect to the vulnerability of our election system, then perhaps you will believe the experts. Unless a computer is always and ever isolated from the internet, any code that is written or viewed on that computer is vulnerable to code manipulation even if the computer is isolated from the internet when the code is loaded to the computer.

You don't have to accept the solution proposed in HB 1390, which in my opinion is the cheapest, quickest, and least vulnerable to manipulation, but you must take action with all due speed to mandate a robust verification count or audit of New Hampshire elections.

I've also provided to the Clerk for the record a summary of the results of a Citizen's Audit in Alegen Michigan which describes a number of error types that can cause machine counts to be inaccurate from paper jams to faint and stray marks causing overvotes that go undetected.

I will be glad to try tp answer any questions you may have.

Post script
MS-ISAC - Multi-state Information Sharing and Analysis Center
CVE - common vulnerabilities and exposures
Cisecurity - Center for Internet Security
EI-ISAC - Elections Infrastructure Information Sharing and Analysis Center