CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-006

Internet Explorer Zero-Day Vulnerability

January 20, 2020 — v1.0

TLP:WHITE

History:

- *20/01/2020 — v1.0 – Initial publication*

Summary

Microsoft released an advisory [1] notifying about a remote code execution (RCE) vulnerability existing in the scripting engine of Internet Explorer (IE). The vulnerability allows an attacker to corrupt the memory of the IE and execute code with the privileges of the current user. Currently, there is no patch for the reported vulnerability.

Technical Details

MS IE Scripting Engine has a memory corruption vulnerability [1] that allows a remote attacker to launch an RCE attack [2]. The execution of the arbitrary code takes place under the session of the current user of the browser. Under certain circumstances the attack can result in a **full system compromise**.

The vulnerability lays in `JScript.dll` and not in `JScript9.dll`. This vulnerability only affects certain websites that utilize `JScript` as the scripting engine.

The vulnerability is registered as CVE-2020-0674 [3].

Affected Products

The vulnerability exists in MS Internet Explorer versions 9/10/11 [1].

Recommendations

No patch is currently available. Please monitor the topic and update as soon as a patch becomes available.

In order to restrict access to `JScript.dll` the following commands can be applied [1]:

- 32-bit systems, execute the following commands with administrator privileges:

```
takeown /f %windir%\system32\jscript.dll
cacls %windir%\system32\jscript.dll /E /P everyone:N
```

- 64-bit systems, execute the following commands with administrator privileges:

```
takeown /f %windir%\syswow64\jscript.dll
cacls %windir%\syswow64\jscript.dll /E /P everyone:N
takeown /f %windir%\system32\jscript.dll
cacls %windir%\system32\jscript.dll /E /P everyone:N
```

These steps might affect the normal functionality of a system and are not resolving the issue, only reduce the possibility of exploitation. Before applying an update, please follow the instructions on the Microsoft Advisory [1] for reverting the access restriction.

IE on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 and Windows Server 2019 runs in a restricted mode that is known as Enhanced Security Configuration. Enhanced Security Configuration is a group of preconfigured settings in Internet Explorer that can reduce the likelihood of a user or administrator downloading and running specially crafted web content on a server. This is a mitigating factor for websites that you have not added to the Internet Explorer Trusted sites zone [1].

References

[1] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200001

[2] https://en.wikipedia.org/wiki/Arbitrary_code_execution

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