Advanced Notification of Cyber Threats against Internet Explorer Injection

Security Advisory	ADV-19-10	**Criticality**	High	○○○●
Advisory Released On	21 March 2019			

Impact

Opening .MHT files using Internet Explorer results in exploitation to .MHT injection vulnerability.

Recommendations

Adhere the advices written under the recommendations section.

Affected Platforms

- Internet Explorer

Summary

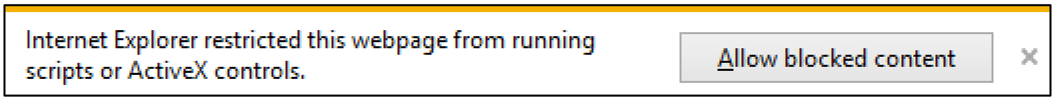
As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a newly discovered threat targeting XXE (XML External Entity) vulnerability in Internet Explorer (IE). This vulnerability is exploited by opening a malicious .MHT file in IE. Immediate exploitation could occur as by default the OS (operating system) suggests opening .MHT files in IE. This factor results in more probable exploitation to the vulnerability. XXE processed by a weak XML parser may lead to various threats, such as disclosure of confidential data, and server side request forgery. Successful exploitation could result in attackers to conduct remote analysis of installed programs on a user machine.

Details

Internet Explorer .MHT injection vulnerability is exploited when a user opens a malicious .MHT file using IE web browser. The .MHT injection vulnerability in IE uses files containing malicious <xml> markup. The factor that results in more probable exploitation to the vulnerability is that IE is suggested by default to open the malicious .MHT files.

Opening a malicious .MHT file without any interaction in IE exploits the vulnerability causing immediate infection. The vulnerability has been tested to extract information remotely to find the program version of some specific installed programs in an infected machine.

IE is a web browser that is installed by default in Windows OS. IE loads local HTML files in the Local Machine Zone. Then, as a security measurement these files typically enable the Local Machine Lockdown feature in IE, creating a warning bar instantiating Active X controls or JavaScript.



Internet Explorer restricted this webpage from running scripts or ActiveX controls.

However, to avoid this security warning, local HTML pages may contain Mark of the web (MOTW). MOTW can be used to avoid the Local Machine Lockdown feature to immediately run content that supposedly should be blocked. MOTW can be assigned using a comment inside HTML markup language or by loading the file from Temporary Internet Files folder. Therefore, when opening a malicious .MHT file using <xml> markup, the users will not get any security warning and the malicious .MHT file will be executed.

XML External Entity (XXE) attack is a type of attack against applications that are able to parse XML inputs. Moreover, IE is an application that has the capabilities to parse XML. As a result, IE is vulnerable to XXE attack and in conjunction with MOTW, the vulnerability is immediately executed without requiring user interaction due to removal of the security bar.

XXE processed by a weak XML parser may lead to various threats, such as disclosure of confidential data, and server side request forgery. Hereafter, XXE processing may be leveraged in .MHT injection vulnerability.

Recommendations

Microsoft have currently no plans to patch this vulnerability as support for Internet Explorer has been discontinued. Therefore, all devices running Internet Explorer are vulnerable and could be exploited.

To avoid the vulnerability, entities are recommended with the following:

- Apply restrictions to disable opening .MHT files.
- Where it is not possible to apply restrictions then advising users to avoid opening .MHT files is highly recommended.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel	(+971) 4 777 4003
Fax	(+971) 4 777 4100
Email	info[at]aeCERT.ae
Instagram	@TheUAETRA
Twitter	@TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae