CERT-EU Security Advisory 2017-004

Arbitrary Code Execution in Internet Explorer and Edge

February 28, 2017 — v1.0

History:

- *28/02/2017 — v1.0: Initial publication*

Summary

Google's Project Zero security research team has disclosed a high-severity vulnerability in Microsoft's Edge and Internet Explorer browsers that reportedly allows attackers to execute malicious code via vectors involving a crafted Cascading Style Sheets (CSS) token sequence and crafted JavaScript code (CVE-2017-0037) [1].

The vulnerability is due to a type confusion issue in one of the functions in `mshtml.dll` (`Layout::MultiColumnBoxBuilder::HandleColumnBreakOnColumnSpanningElement`). An attacker that can convince an affected user to visit an attacker-controlled web page or to open a crafted HTML page with the affected browser, could exploit the vulnerability. If successful, the attacker could execute arbitrary code on the targeted system with the privileges of the affected browser [2].

Products Affected

This vulnerability affects all versions of Internet Explorer 11 and Microsoft's Edge on Windows systems.

Project Zero researcher Ivan Fratric reported the bug to Microsoft on 25/11/2016. It was made public on 28/02/2017, in line with Google's policy of publishing vulnerability details 90 days after being privately reported [2].

Recommendations

As no patch is available yet, it is highly recommended to avoid using Internet Explorer 11 or Microsoft's Edge on Windows for the time being. Microsoft has not provided a date for a patch release.

References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0037

[2] https://bugs.chromium.org/p/project-zero/issues/detail?id=1011