NCSC
National Cyber Security Centre

2109081241-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Microsoft MSHTML Remote Code Execution Vulnerability (CVE-2021-40444) - UPDATE
2021-09-14

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Revision History

Revision	Date	Author(s)	Description
1.0	08 August 2021	CSIRT-IE	Initial Alert created regarding MSHTML Vulnerability (NCSC MSHTML Advisory)
1.1	14 September 2021	CSIRT-IE	Security Patch released by Microsoft

MSHTML Vulnerability

Threat Type	A vulnerability exists in MSHTML which is a part of all versions of Microsoft Windows. The vulnerability (CVE-2021-40444) may allow attackers to craft a malicious ActiveX control to be used by a Microsoft Office document that hosts the browser rendering engine. This document would then be used as part of a spear-phishing campaign. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. The NCSC has been advised that this technique is being exploited by malicious actors.
Products Affected	All versions of Microsoft Windows.
Impact	Remote Code Execution - compromised systems, data loss.
Mitigations	By default, Microsoft Office opens documents from the internet in Protected View or Application Guard for Office both of which prevent the current attack. Disabling the installation of all ActiveX controls in Internet Explorer mitigates this attack. This can be accomplished for all sites by updating the registry. Previously-installed ActiveX controls will continue to run, but do not expose this vulnerability. See the Microsoft Advisory for full mitigation steps.
Recommendations	**UPDATE:** Microsoft has released security updates to address this vulnerability. The NCSC recommends that affected organisations review the Security Updates table for the relevant update for your system and apply it as soon as possible.

DISCLAIMER: *This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie