MSRC > Customer Guidance > Security Update Guide > Vulnerabilities > CVE 2021 40444

Microsoft MSHTML Remote Code Execution Vulnerability

On this page

Subscribe RSS PowerShell {} API

CVE-2021-40444
Security Vulnerability

Released: Sep 7, 2021

Last updated: Aug 16, 2022

Assigning CNA: Microsoft

CVE-2021-40444

CVSS:3.0 8.8 / 7.9

Expand all Collapse all

Metric	Value
Base score metrics (8)	
▶ Attack Vector	▶ Network
▶ Attack Complexity	▶ Low
▶ Privileges Required	▶ None
▶ User Interaction	▶ Required
▶ Scope	▶ Changed
▶ Confidentiality	▶ Low
▶ Integrity	▶ High
▶ Availability	▶ Low
Temporal score metrics (3)	
▶ Exploit Code Maturity	▶ Proof-of-Concept
▶ Remediation Level	▶ Official Fix
▶ Report Confidence	▶ Confirmed

Please see Common Vulnerability Scoring System for more information on the definition of these metrics.

Executive Summary

Microsoft is investigating reports of a remote code execution vulnerability in MSHTML that affects Microsoft Windows. Microsoft is aware of targeted attacks that attempt to exploit this vulnerability by using specially-crafted Microsoft Office documents.

An attacker could craft a malicious ActiveX control to be used by a Microsoft Office document that hosts the browser rendering engine. The attacker would then have to convince the user to open the malicious document. 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.

Microsoft Defender Antivirus and Microsoft Defender for Endpoint both provide detection and protections for the known vulnerability. Customers should keep antimalware products up to date. Customers who utilize automatic updates do not need to take additional action. Enterprise customers who manage updates should select the detection build 1.349.22.0 or newer and deploy it across their environments. Microsoft Defender for Endpoint alerts will be displayed as: "Suspicious Cpl File Execution".

Upon completion of this investigation, Microsoft will take the appropriate action to help protect our customers. This may include providing a security update