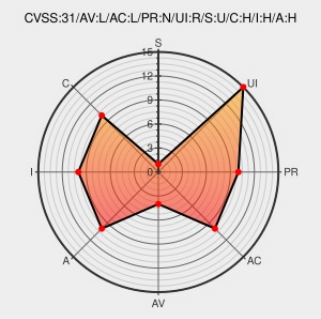
CVE-2021-40486

Published on: 10/12/2021 12:00:00 AM UTC

Last Modified on: 10/19/2021 03:44:00 PM UTC

CVE-2021-40486

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Office from Microsoft contain the following vulnerability:

Microsoft Word Remote Code Execution Vulnerability

CVE-2021-40486 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
ZDI-21-1158 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-1158/
Security Update Guide - Microsoft Security Response Center	portal.msrc.microsoft.com text/html	MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40486

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

110392 Microsoft SharePoint Enterprise Server Multiple Vulnerabilities October 2021

110393 Microsoft Office and Microsoft Office Services and Web Apps Security Update October 2021

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Office	2019	All	All	All
Application	Microsoft	Office Online Server	-	All	All	All
Application	Microsoft	Office Web Apps Server	2013	sp1	All	All
Application	Microsoft	Sharepoint Enterprise Server	2013	sp1	All	All
Application	Microsoft	Sharepoint Enterprise Server	2016	All	All	All
Application	Microsoft	Sharepoint Server	2019	All	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word	2013	sp1	All	All
Application	Microsoft	Word	2016	All	All	All

cpe:2.3:a:microsoft:office:2019:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office_online_server:-:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:office_web_apps_server:2013:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sharepoint_enterprise_server:2013:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sharepoint_enterprise_server:2016:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:word:2013:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:word:2013:sp1:*:*:rt:*:*:*:

cpe:2.3:a:microsoft:word:2016:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/u/Hackburg	Update Your Windows PCs Immediately To Patch New 0-Day Under Active Attack.	2021-10-14

01:47:13

← Previous ID

Next ID→

© CVE.report 2021 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report