



CVE-2017-11935

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-11935
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-12 21:29:00 UTC
Updated	2017-12-27 16:09:00 UTC
Description	Microsoft Office 2016 Click-to-Run (C2R) allows a remote code execution vulnerability due to the way files are handled in r

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Office	2016	c2r	All	All
Application	Microsoft	Office	2016	c2r	All	All

References

Reference	Source	Link
Microsoft Excel CVE-2017-11935 Remote Code Execution Vulnerability	BID	www.securityfocus.com/bid/79844
Microsoft Office Excel File Processing Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTrack	www.securitytracker.com/id?1037544
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11935	CONFIRM	portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11935
CVE Program record	CVE.ORG	www.cve.org/CVERecord/CVE-2017-11935
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2017-11935

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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 registered 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](#).

Free CVE JSON API cve.report/api

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