



CVE-2019-1385

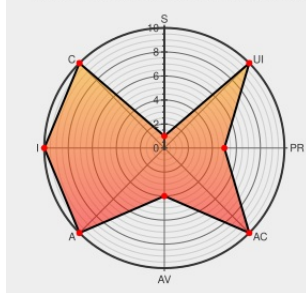
Published on: 11/12/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:48 PM UTC

CVE-2019-1385

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Windows 10](#) from [Microsoft](#) contain the following vulnerability:

An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files. To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges. The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'.

CVE-2019-1385 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	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.1 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	COMPLETE

CVE References

Description	Tags	Link
Security Update Guide - Microsoft Security	CVE-2019-1385	MSRC notal page microsoft.com/en-US/security

Security Update Guide - Microsoft Security Response Center

Patch

Vendor Advisory

portal.msrc.microsoft.com

text/html

 MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1385

ZDI-19-979 | Zero Day Initiative

Third Party Advisory

www.zerodayinitiative.com

text/html

 MISC www.zerodayinitiative.com/advisories/ZDI-19-979/

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.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Enjoy hacking ;)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	All	All	All
Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All
Operating System	Microsoft	Windows 10	1809	All	All	All
Operating System	Microsoft	Windows 10	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All

Operating System	Microsoft	Windows Server 2019	-	All	All	All
cpe:2.3:o:microsoft:windows_10:1709:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_10:1803:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_10:1809:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_10:1903:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_10:1709:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_10:1803:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_10:1809:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_10:1903:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_server_2016:1803:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_server_2016:1903:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_server_2016:1803:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_server_2016:1903:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_server_2019:-::~~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:microsoft:windows_server_2019:-::~~::~~::~~::~~::~~::~~::~~::						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		