



CVE-2019-0666

Published on: 04/08/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:02 PM UTC

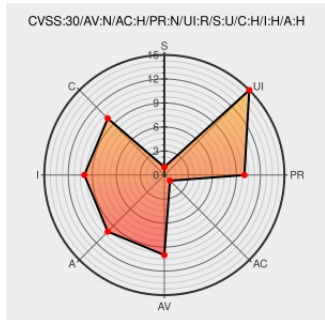
CVE-2019-0666

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Internet Explorer](#) from [Microsoft](#) contain the following vulnerability:

A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0665, CVE-2019-0667, CVE-2019-0772.

CVE-2019-0666 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **7.6 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
No Description Provided	Patch Vendor Advisory portal.msrc.microsoft.com text/html	CONFIRM portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0666

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Internet Explorer	10	All	All	All
Application	Microsoft	Internet Explorer	11	-	All	All
Application	Microsoft	Internet Explorer	9	All	All	All
Application	Microsoft	Internet Explorer	10	All	All	All
Application	Microsoft	Internet Explorer	11	-	All	All
Application	Microsoft	Internet Explorer	9	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1703	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	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1703	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 7	-	sp1	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All

Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
cpe:2.3:a:microsoft:internet_explorer:10:*:*:*:*:*:						
cpe:2.3:a:microsoft:internet_explorer:11:*:*:*:*:*:						
cpe:2.3:a:microsoft:internet_explorer:9:*:*:*:*:*:						
cpe:2.3:a:microsoft:internet_explorer:10:*:*:*:*:*:						
cpe:2.3:a:microsoft:internet_explorer:11:*:*:*:*:*:						
cpe:2.3:a:microsoft:internet_explorer:9:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:1703:*:*:*:*:*:						

```
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:-:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows 10:1607:*.:.:.:.:.:
```

```
cpe:2.3:o:microsoft:windows_10:1703:*:*:*:*:*:*:
```

```
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 7:-sp1:*.:.:.:.:
```

```
cpe:2.3:o:microsoft:windows_7:-:sp1:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows 8.1:-:*:*:*:*:*:
```

cpe:2.3:o:microsoft:windows 8.1:-:*:*:*:*:*:*

```
cpe:2.3:o:microsoft:windows rt 8.1:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_rt 8.1:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:x64:*
```

```
cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*.:.:.:.:
```

```
cpe:2.3:o:microsoft:windows server 2008:r2:sp1:*:*:*:x64:*
```

```
cpe:2.3:o:microsoft:windows server 2012:-:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2012:r2:::*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows server 2012:r2:::*:*:*.*
```

```
cpe:2.3:o:microsoft:windows server 2016:-:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:
```

Social Mentions		
Source	Title	Posted (UTC)
 @DirectoryRanger	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys...	2021-03-29 07:40:53
 @ptracesecurity	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #Pentesting #CVE #RCE #CyberSecurity... twitter.com/i/web/status/1...	2021-03-30 05:52:27
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #infosec	2021-03-30 11:29:04
 @Anastasis_King	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #Pentesting #CVE #RCE #CyberSecurity #Infosec	2021-03-30 20:22:11
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #CyberSecurity #security	2021-04-06 13:40:14
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #security #MalwareAnalysis	2021-04-12 17:49:47
 @ptracesecurity	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #Pentesting #Vulnerability #CVE... twitter.com/i/web/status/1...	2021-04-16 16:41:05
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #CyberSecurity #infosec	2021-04-25 07:43:31
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #MalwareAnalysis #infosec	2021-05-01 05:48:13
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #CyberSecurity	2021-05-07 21:24:03
 @reverseame	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys...	2021-05-10 13:38:04
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #InfomationSecurity #security	2021-05-14 12:56:59
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #CyberSecurity #infosec	2021-05-21 17:28:19
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #infosec #MalwareAnalysis	2021-05-28 07:17:36
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #InfomationSecurity #security	2021-06-05 02:53:32
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #CyberSecurity #InfomationSecurity	2021-06-11 03:09:32
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #MalwareAnalysis #CyberSecurity	2021-06-18 03:49:50
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #CyberSecurity #infosec	2021-06-25 14:52:28
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #InfomationSecurity #MalwareAnalysis	2021-07-04 22:02:16
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #InfomationSecurity #CyberSecurity	2021-07-13 17:38:32
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analys... #analysis #CyberSecurity #infosec	2021-07-24 22:37:23

 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analysis... #analysis #InformationSecurity #security	2021-08-03 21:06:48
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analysis... #analysis #CyberSecurity #infosec	2021-08-13 12:12:46
 @MaltrakN	Analysis of a VB Script Heap Overflow (CVE-2019-0666) malwaretech.com/2019/04/analysis... #analysis #infosec #MalwareAnalysis	2021-08-23 08:31:26

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)