



CVE-2020-0665

Published on: 02/11/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-0665

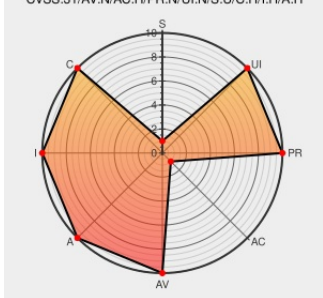
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:31/AV:N/AC:H/PR:N/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 in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'.

CVE-2020-0665 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
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
No Description Provided	Patch Vendor Advisory portal.msrc.microsoft.com text/html	portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0665

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
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	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 10	1909	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	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	1909	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


```
cpe:2.3:o:microsoft:windows_10:1607:::~::~:
```

```
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_10:1909:*.:.:.:.:.:
```

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

```
cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:
```

```
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_10:1909:*:*:*:*:*:*:
```

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

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

```
cpe:2.3:0:microsoft:windows_8.1:-:*:*:*:*:*:*:
```

```
cpe:2.3:0: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:*:*:*:itanium:*:

```
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:*:*:*:itanium:*:

```
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_2016:1803:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2016:1903:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2016:1909:*:*:*:*:*:
cpe:2.3:o:microsoft:windows_server_2016:-:*:*:*:*:*:
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_2016:1909:*:*:*:*:*:
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

Social Mentions		
Source	Title	Posted (UTC)
 @zunil2_test	面白かった。別フォレストにある標的サーバのローカルSIDを自フォレスト情報として伝えることで、SID Filteringをスルーしてそのサーバに管理者アクセスできるみたいなやつ。この問題はCVE-2020-0665として対策済... twitter.com/i/web/status/1...	2021-05-29 04:25:29