



# CVE-2016-0180

Published on: 05/10/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:13 PM UTC

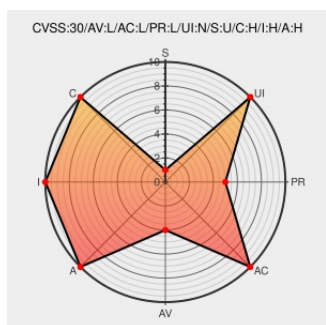
## CVE-2016-0180

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles symbolic links, which allows local users to gain privileges via a crafted application, aka "Windows Kernel Elevation of Privilege Vulnerability."

CVE-2016-0180 has been assigned by [secure@microsoft.com](mailto: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    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.2 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>LOCAL</b>           | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                                                                                              | Tags                                                                 | Link                    |
|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-------------------------|
| Windows Kernel Symbolic Link Processing Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker | <a href="#">www.securitytracker.com</a><br><a href="#">text/html</a> | <a href="#">1035833</a> |

Microsoft Security Bulletin MS16-060 - Important | Microsoft Docs

docs.microsoft.com

text/html

 MS MS16-060

Microsoft Windows Kernel CVE-2016-0180 Local Privilege Escalation Vulnerability

cve.report (archive)

text/html

 BID 90028

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](mailto: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     | All      |
| Operating System                         | Microsoft | Windows 10          | 1511    | All    | All     | All      |
| Operating System                         | Microsoft | Windows 10          | All     | All    | All     | All      |
| Operating System                         | Microsoft | Windows 10          | 1511    | All    | All     | All      |
| Operating System                         | Microsoft | Windows 7           | All     | sp1    | All     | All      |
| Operating System                         | Microsoft | Windows 7           | -       | sp1    | x86     | All      |
| Operating System                         | Microsoft | Windows 7           | All     | sp1    | All     | All      |
| Operating System                         | Microsoft | Windows 7           | -       | sp1    | x86     | All      |
| Operating System                         | Microsoft | Windows 8.1         | All     | All    | All     | All      |
| Operating System                         | Microsoft | Windows 8.1         | All     | All    | All     | All      |
| Operating System                         | Microsoft | Windows Rt 8.1      | All     | All    | All     | All      |
| Operating System                         | Microsoft | Windows Rt 8.1      | All     | All    | All     | All      |
| Operating System                         | Microsoft | Windows Server 2008 | All     | sp2    | All     | All      |
| Operating System                         | Microsoft | Windows Server 2008 | r2      | sp1    | All     | All      |
| Operating System                         | Microsoft | Windows Server 2008 | All     | sp2    | All     | All      |
| Operating System                         | Microsoft | Windows Server 2008 | r2      | sp1    | All     | All      |

|                                                       |           |                     |     |     |     |     |
|-------------------------------------------------------|-----------|---------------------|-----|-----|-----|-----|
| Operating System                                      | Microsoft | Windows Server 2012 | All | All | All | All |
| Operating System                                      | Microsoft | Windows Server 2012 | r2  | All | All | All |
| Operating System                                      | Microsoft | Windows Server 2012 | All | All | All | All |
| Operating System                                      | Microsoft | Windows Server 2012 | r2  | All | All | All |
| Operating System                                      | Microsoft | Windows Vista       | All | sp2 | All | All |
| Operating System                                      | Microsoft | Windows Vista       | All | sp2 | All | All |
| cpe:2.3:o:microsoft:windows_10:*****:                 |           |                     |     |     |     |     |
| cpe:2.3:o:microsoft:windows_10:1511:*****:            |           |                     |     |     |     |     |
| cpe:2.3:o:microsoft:windows_10:*****:                 |           |                     |     |     |     |     |
| cpe:2.3:o:microsoft:windows_10:1511:*****:            |           |                     |     |     |     |     |
| cpe:2.3:o:microsoft:windows_7:*:sp1:*****:            |           |                     |     |     |     |     |
| cpe:2.3:o:microsoft:windows_7:-:sp1:x86:*****:        |           |                     |     |     |     |     |
| cpe:2.3:o:microsoft:windows_7:*:sp1:*****:            |           |                     |     |     |     |     |
| cpe:2.3:o:microsoft:windows_7:-:sp1:x86:*****:        |           |                     |     |     |     |     |
| 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:*****: |           |                     |     |     |     |     |
| cpe:2.3:o:microsoft:windows_server_2008:*:sp2:*****:  |           |                     |     |     |     |     |
| cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*****: |           |                     |     |     |     |     |
| 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_vista:*:sp2:*****:        |           |                     |     |     |     |     |

```
cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:*:
```

[← Previous ID](#)

© CVE.report 2023   |

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](https://status.cve.report)