



# CVE-2018-8484

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

## Summary

|                        |                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2018-8484                                                                                                             |
| <b>State</b>           | PUBLIC                                                                                                                    |
| <b>Assigner</b>        | secure@microsoft.com                                                                                                      |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                              |
| <b>Published</b>       | 2018-10-10 13:29:00 UTC                                                                                                   |
| <b>Updated</b>         | 2019-10-03 00:03:00 UTC                                                                                                   |
| <b>Description</b>     | An elevation of privilege vulnerability exists when the DirectX Graphics Kernel (DXGKRNL) driver improperly handles objec |

## Risk And Classification

### Problem Types: CWE-404

## NVD Known Affected Configurations (CPE 2.3)

| 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     | 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     | All      |
| Operating System | Microsoft | Windows 8.1    | All     | All    | All     | All      |
| Operating System | Microsoft | Windows Rt 8.1 | -       | All    | All     | All      |

|                  |                           |                                     |      |     |     |     |
|------------------|---------------------------|-------------------------------------|------|-----|-----|-----|
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Rt 8.1</a>      | -    | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2012</a> | -    | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2012</a> | r2   | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2012</a> | -    | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2012</a> | r2   | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2016</a> | -    | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2016</a> | 1709 | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2016</a> | 1803 | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2016</a> | -    | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2016</a> | 1709 | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2016</a> | 1803 | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2019</a> | -    | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows Server 2019</a> | -    | All | All | All |

References

| Reference                                                                                                                             | Sou |
|---------------------------------------------------------------------------------------------------------------------------------------|-----|
| Microsoft GDI+ Multiple Bugs Lets Local Users Gain Potentially Sensitive Information and Obtain Elevated Privileges - SecurityTracker | SEC |
| portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8484                                                              | COM |
| Microsoft Windows DirectX Graphics Kernel CVE-2018-8484 Local Privilege Escalation Vulnerability                                      | BID |
| CVE Program record                                                                                                                    | CVE |
| NVD vulnerability detail                                                                                                              | NVD |

No vendor comments have been submitted for this CVE.

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