



CVE-2018-8176

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2018-8176 |
| State | PUBLIC |
| Assigner | secure@microsoft.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-05-23 13:29:00 UTC |
| Updated | 2018-06-05 18:40:00 UTC |
| Description | A remote code execution vulnerability exists in Microsoft PowerPoint software when the software fails to properly validate X |

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-----------|----------------|---------|--------|---------|----------|
| Application | Microsoft | Office For Mac | 2016 | All | All | All |
| Application | Microsoft | Office For Mac | 2016 | All | All | All |

References

| Reference | Source | Link |
|---|----------|--------------------|
| portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8176 | CONFIRM | portal.msrc.micros |
| Microsoft PowerPoint CVE-2018-8176 Remote Code Execution Vulnerability | BID | www.securityfocus |
| Microsoft PowerPoint XML Processing Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker | SECTRACK | www.securitytrack |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API [cve.report/api](#)

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