



CVE-2015-6097

Published on: 11/11/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6097

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Windows 7](#) from [Microsoft](#) contain the following vulnerability:

Heap-based buffer overflow in Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted Journal (.jnt) file, aka "Windows Journal Heap Overflow Vulnerability."

CVE-2015-6097 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Windows Journal File Processing Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker

www.securitytracker.com
text/html

[SECTrack 1034110](#)

Verisign is a global provider of domain name registry services and internet infrastructure - Verisign

www.verisign.com
text/xml

[IDEFENSE 20151201 Microsoft Windows Journal Heap Overflow Vulnerability](#)

Microsoft Security Bulletin MS15-114 - Critical | Microsoft Docs

docs.microsoft.com
text/html

[MS MS15-114](#)

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 7	-	sp1	All	All
Operating System	Microsoft	Windows 7	-	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 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All

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

```
cpe:2.3:o:microsoft:windows_7:-: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_2008:-:sp2:*:*:*:*:*:
```

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

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

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

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report