

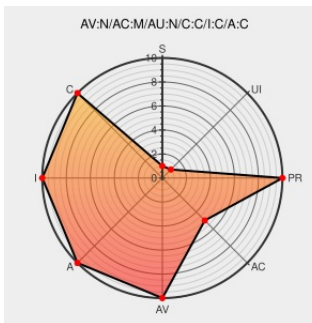


CVE-2013-3157

Published on: 09/11/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:31 PM UTC

CVE-2013-3157

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

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

Microsoft Access 2007 SP3, 2010 SP1 and SP2, and 2013 in Microsoft Office allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Access file, aka "Access Memory Corruption Vulnerability," a different vulnerability than CVE-2013-3155.

CVE-2013-3157 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Microsoft Security Bulletin MS13-074 - Important Microsoft Docs	docs.microsoft.com text/html	MS MS13-074
Microsoft Updates for Multiple Vulnerabilities US-CERT	US Government Resource www.us-cert.gov text/html	CERT TA13-253A
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval.org/mitre/oval:def:18664

By selecting these links, you may be leaving CVEreport workspace. 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
Application	Microsoft	Access	2007	sp3	All	All
Application	Microsoft	Access	2010	sp1	All	All
Application	Microsoft	Access	2010	sp1	All	All
Application	Microsoft	Access	2010	sp2	All	All
Application	Microsoft	Access	2010	sp2	All	All
Application	Microsoft	Access	2013	All	All	All
Application	Microsoft	Access	2013	All	All	All
Application	Microsoft	Access	2007	sp3	All	All
Application	Microsoft	Access	2010	sp1	All	All
Application	Microsoft	Access	2010	sp1	All	All
Application	Microsoft	Access	2010	sp2	All	All
Application	Microsoft	Access	2010	sp2	All	All
Application	Microsoft	Access	2013	All	All	All
Application	Microsoft	Access	2013	All	All	All

```
cpe:2.3:a:microsoft:access:2007:sp3:*:*:*:*:*
```

```
cpe:2.3:a:microsoft:access:2010:sp1:*:*:*:x64*.*
```

cpe:2.3:a:microsoft:access:2010:sp1:*:*:x86:*.*:

cpe:2.3:a:microsoft:access:2010:sp2:*:*:*:x64.*:

cpe:2.3:a:microsoft:access:2010:sp2:*:*:x86:*.*

```
cpe:2.3:a:microsoft:access:2013:*:*:*:*:*.x64.*:
```

```
cpe:2.3:a:microsoft:access:2013:*:*:*:x86:*:
```

```
cpe:2.3:a:microsoft:access:2007:sp3:*:*:*:*:
```

```
cpe:2.3:a:microsoft:access:2010:sp1:*:*:*:x64:*:
```

```
cpe:2.3:a:microsoft:access:2010:sp1:*:*:x86:*:*
```

```
cpe:2.3:a:microsoft:access:2010:sp2:*:*:*:x64:*:
```

```
cpe:2.3:a:microsoft:access:2010:sp2:*:*:x86:*.*:
```

```
cpe:2.3:a:microsoft:access:2013:*.~*~*~*~*.x64.*:
```

cpe:2.3:a:microsoft:access:2013:*:*:*:x86:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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