

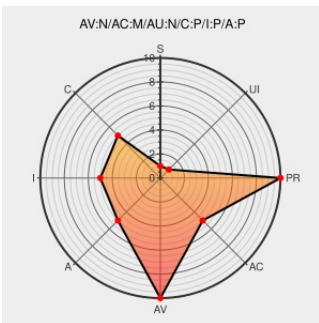


# CVE-2010-3786

Published on: 11/16/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:02 PM UTC

## CVE-2010-3786

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

Certain versions of [Mac Os X](#) from [Apple](#) contain the following vulnerability:

QuickLook in Apple Mac OS X 10.6.x before 10.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted Excel file.

CVE-2010-3786 has been assigned by [product-security@apple.com](mailto:product-security@apple.com) to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access  
Vector

**NETWORK**

Access  
Complexity

**MEDIUM**

Authentication

**NONE**

Confidentiality  
Impact

**PARTIAL**

Integrity  
Impact

**PARTIAL**

Availability  
Impact

**PARTIAL**

## CVE References

Description

Tags

Link

APPLE-SA-2010-11-10-1 Mac OS X v10.6.5 and Security Update 2010-007

[Vendor Advisory](#)  
[lists.apple.com](#)  
[text/html](#)

[APPLE APPLE-SA-2010-11-10-1](#)

Apple iOS Multiple Vulnerabilities - Advisories - Community

[web.archive.org](#)  
[text/html](#)

[SECUNIA 42314](#)

About the security content of Numbers for iOS v1.5

[support.apple.com](#)  
[text/html](#)

[CONFIRM support.apple.com/kb/HT5004](#)

Mac OS X Lets Remote Users Execute Arbitrary Code, Deny Service, and Obtain Information - SecurityTracker

[www.securitytracker.com](#)  
[text/html](#)

[SECTRACK 1024723](#)

APPLE-SA-2011-10-12-6 Numbers for iOS v1.5

[lists.apple.com](#)  
[text/html](#)

[APPLE APPLE-SA-2011-10-12-6](#)

Webmail : Solution de messagerie professionnelle -

[www.vupen.com](#)

[VUPEN ADV-2010-3046](#)

|                                                                             |                                                                                                                                                                                        |                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OVHcloud- OVH                                                               | <a href="#">text/html</a>                                                                                                                                                              |                                                                                                                                                                                                         |
| About the security content of iOS 4.2                                       | <a href="#">support.apple.com</a><br><a href="#">text/html</a>                                                                                                                         |  <a href="#">CONFIRM support.apple.com/kb/HT4456</a>                                                                 |
| APPLE-SA-2010-11-22-1 iOS 4.2                                               | <a href="#">lists.apple.com</a><br><a href="#">text/html</a>                                                                                                                           |  <a href="#">APPLE APPLE-SA-2010-11-22-1</a>                                                                         |
| Public Advisory: 11.11.10 // iDefense Labs                                  | <a href="#">web.archive.org</a><br><a href="#">text/html</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a>                                                             |  <a href="#">IDEFENSE 20101111 Apple Mobile OfficeImport Framework Excel Parsing Memory Corruption Vulnerability</a> |
| About the security content of Mac OS X v10.6.5 and Security Update 2010-007 | <a href="#">Patch</a><br><a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> |  <a href="#">CONFIRM support.apple.com/kb/HT4435</a>                                                                 |

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 | <a href="#">Apple</a> | <a href="#">Mac Os X</a>        | 10.6.0  | All    | All     | All      |
| Operating System | <a href="#">Apple</a> | <a href="#">Mac Os X</a>        | 10.6.1  | All    | All     | All      |
| Operating System | <a href="#">Apple</a> | <a href="#">Mac Os X</a>        | 10.6.2  | All    | All     | All      |
| Operating System | <a href="#">Apple</a> | <a href="#">Mac Os X</a>        | 10.6.3  | All    | All     | All      |
| Operating System | <a href="#">Apple</a> | <a href="#">Mac Os X</a>        | 10.6.4  | All    | All     | All      |
| Operating System | <a href="#">Apple</a> | <a href="#">Mac Os X</a>        | 10.6.0  | All    | All     | All      |
| Operating System | <a href="#">Apple</a> | <a href="#">Mac Os X</a>        | 10.6.1  | All    | All     | All      |
| Operating System | <a href="#">Apple</a> | <a href="#">Mac Os X</a>        | 10.6.2  | All    | All     | All      |
| Operating System | <a href="#">Apple</a> | <a href="#">Mac Os X</a>        | 10.6.3  | All    | All     | All      |
| Operating System | <a href="#">Apple</a> | <a href="#">Mac Os X</a>        | 10.6.4  | All    | All     | All      |
| Operating System | <a href="#">Apple</a> | <a href="#">Mac Os X Server</a> | 10.6.0  | All    | All     | All      |
| Operating System | <a href="#">Apple</a> | <a href="#">Mac Os X Server</a> | 10.6.1  | All    | All     | All      |



cpe:2.3:o:apple:mac\_os\_x\_server:10.6.3:\*\*\*\*\*:

cpe:2.3:o:apple:mac\_os\_x\_server:10.6.4:\*\*\*\*\*:

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](#)