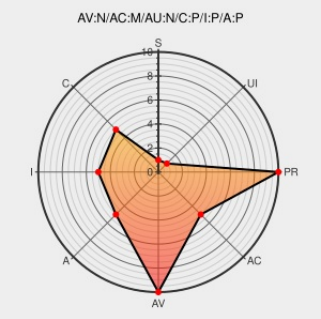
CVE-2011-0175

Published on: 03/22/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:18 PM UTC

CVE-2011-0175

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mac Os X from Apple contain the following vulnerability:

Multiple buffer overflows in Apple Type Services (ATS) in Apple Mac OS X before 10.6.7 allow remote attackers to execute arbitrary code via a document that contains a crafted embedded TrueType font.

CVE-2011-0175 has been assigned by product-security@apple.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
APPLE-SA-2011-03-21-1 Mac OS X v10.6.7 and Security Update 2011-001	Patch, Vendor Advisory, lists.apple.com, text/html	APPLE APPLE-SA-2011-03-21-1
About the security content of Mac OS X v10.6.7 and Security Update 2011-001	Patch, Vendor Advisory, support.apple.com, text/html	CONFIRM support.apple.com/kb/HT4581

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	10.6.0	All	All	All
Operating System	Apple	Mac Os X	10.6.1	All	All	All
Operating System	Apple	Mac Os X	10.6.2	All	All	All
Operating System	Apple	Mac Os X	10.6.3	All	All	All
Operating System	Apple	Mac Os X	10.6.4	All	All	All
Operating System	Apple	Mac Os X	10.6.5	All	All	All
Operating System	Apple	Mac Os X	10.6.0	All	All	All
Operating System	Apple	Mac Os X	10.6.1	All	All	All
Operating System	Apple	Mac Os X	10.6.2	All	All	All
Operating System	Apple	Mac Os X	10.6.3	All	All	All
Operating System	Apple	Mac Os X	10.6.4	All	All	All
Operating System	Apple	Mac Os X	10.6.5	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X Server	10.6.0	All	All	All
Operating System	Apple	Mac Os X Server	10.6.1	All	All	All
Operating System	Apple	Mac Os X Server	10.6.2	All	All	All
Operating System	Apple	Mac Os X Server	10.6.3	All	All	All
Operating System	Apple	Mac Os X Server	10.6.4	All	All	All
Operating System	Apple	Mac Os X Server	10.6.5	All	All	All
Operating System	Apple	Mac Os X Server	10.6.0	All	All	All
Operating System	Apple	Mac Os X Server	10.6.1	All	All	All

Operating System	Apple	Mac Os X Server	10.6.1	All	All	All
Operating System	Apple	Mac Os X Server	10.6.2	All	All	All
Operating System	Apple	Mac Os X Server	10.6.3	All	All	All
Operating System	Apple	Mac Os X Server	10.6.4	All	All	All
Operating System	Apple	Mac Os X Server	10.6.5	All	All	All
Operating System	Apple	Mac Os X Server	All	All	All	All

cpe:2.3:o:apple:mac_os_x:10.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.6.2:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.6.3:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.6.4:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.6.5:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.6.2:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.6.3:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.6.4:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.6.5:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x_server:10.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x_server:10.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x_server:10.6.2:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x_server:10.6.3:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x_server:10.6.4:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x_server:10.6.5:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x_server:10.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x_server:10.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x_server:10.6.2:*:*:*:*:*:*:*

cpe:2.3:o:apple:mac_os_x_server:10.6.3:*:*:*:*:*:*:*

cpe:2.3:o:apple:mac_os_x_server:10.6.4:*:*:*:*:*:*:*

cpe:2.3:o:apple:mac_os_x_server:10.6.5:*:*:*:*:*:*:*

cpe:2.3:o:apple:mac_os_x_server:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→