

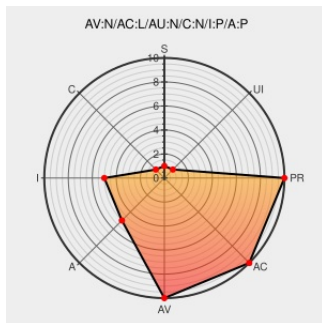


CVE-2006-1983

Published on: 04/21/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

CVE-2006-1983

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

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

Multiple heap-based buffer overflows in Mac OS X 10.4.6 and earlier allow remote attackers to cause a denial of service and possibly execute arbitrary code via the (1) PredictorVSetField function for TIFF or (2) CFAllocatorAllocate function for GIF, as used in applications that use ImageIO or AppKit. NOTE: the BMP vector has been re-assigned to CVE-2006-2238 because it affects a separate product family.

CVE-2006-1983 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Apple Mac OS X Security Update 2006-003 Multiple Vulnerabilities

[cve.report \(archive\)](#)
[text/html](#)

[🌐 BID 17951](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[Vendor Advisory](#)
[www.vupen.com](#)
[text/html](#)

[🌐 VUPEN ADV-2006-1779](#)

No Description Provided

[www.osvdb.org](#)

[🌐 OSVDB 24821](#)

Inactive Link **Not Archived**

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[🔗 XF macosx-cfallocatorallocate-bo\(25949\)](#)

Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-1452
APPLE-SA-2006-05-11 Security Update 2006-003	Patch lists.apple.com text/html	APPLE APPLE-SA-2006-05-11
Security-Protocols :: Computer Security Research	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.security-protocols.com/sp-x28-advisory.php
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF macosx-predictorvsetfield-bo(25951)
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 20077
No Description Provided	Exploit www.security-protocols.com text/html Inactive Link Not Archived	MISC www.security-protocols.com/modules.php?name=News&file=article&sid=3233
US-CERT Technical Cyber Security Alert TA06-132A -- Apple Mac Products Affected by Multiple Vulnerabilities	Patch Third Party Advisory US Government Resource www.us-cert.gov text/html	CERT TA06-132A
Security-Protocols :: Computer Security Research	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.security-protocols.com/sp-x30-advisory.php
Apple Mac OS X Multiple Security Vulnerabilities	Exploit cve.report (archive) text/html	BID 17634
SecurityTracker.com Archives - Apple QuickTime Buffer Overflows in Processing JPEG/BMP/FlashPix/PICT Images and QuickTime/AVI/MPEG4/Flash Movies Let Remote Users Execute Arbitrary Code	Patch securitytracker.com text/html	SECTrack 1016067
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24822
Mac OS X Multiple Potential Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 19686

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	Editor	Language
------	--------	---------	---------	--------	--------	----------

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac OS X	10.3	All	All	All
Operating System	Apple	Mac OS X	10.3.1	All	All	All
Operating System	Apple	Mac OS X	10.3.2	All	All	All
Operating System	Apple	Mac OS X	10.3.3	All	All	All
Operating System	Apple	Mac OS X	10.3.4	All	All	All
Operating System	Apple	Mac OS X	10.3.5	All	All	All
Operating System	Apple	Mac OS X	10.3.6	All	All	All
Operating System	Apple	Mac OS X	10.3.7	All	All	All
Operating System	Apple	Mac OS X	10.3.8	All	All	All
Operating System	Apple	Mac OS X	10.3.9	All	All	All
Operating System	Apple	Mac OS X	10.4	All	All	All
Operating System	Apple	Mac OS X	10.4.1	All	All	All
Operating System	Apple	Mac OS X	10.4.2	All	All	All
Operating System	Apple	Mac OS X	10.4.3	All	All	All
Operating System	Apple	Mac OS X	10.4.4	All	All	All
Operating System	Apple	Mac OS X	10.4.5	All	All	All
Operating System	Apple	Mac OS X	10.4.6	All	All	All
Operating System	Apple	Mac OS X	10.3	All	All	All
Operating System	Apple	Mac OS X	10.3.1	All	All	All
Operating System	Apple	Mac OS X	10.3.2	All	All	All
Operating System	Apple	Mac OS X	10.3.3	All	All	All
Operating System	Apple	Mac OS X	10.3.4	All	All	All
Operating System	Apple	Mac OS X	10.3.5	All	All	All

System						
Operating System	Apple	Mac Os X	10.3.6	All	All	All
Operating System	Apple	Mac Os X	10.3.7	All	All	All
Operating System	Apple	Mac Os X	10.3.8	All	All	All
Operating System	Apple	Mac Os X	10.3.9	All	All	All
Operating System	Apple	Mac Os X	10.4	All	All	All
Operating System	Apple	Mac Os X	10.4.1	All	All	All
Operating System	Apple	Mac Os X	10.4.2	All	All	All
Operating System	Apple	Mac Os X	10.4.3	All	All	All
Operating System	Apple	Mac Os X	10.4.4	All	All	All
Operating System	Apple	Mac Os X	10.4.5	All	All	All
Operating System	Apple	Mac Os X	10.4.6	All	All	All
Operating System	Apple	Mac Os X Server	10.3	All	All	All
Operating System	Apple	Mac Os X Server	10.3.1	All	All	All
Operating System	Apple	Mac Os X Server	10.3.2	All	All	All
Operating System	Apple	Mac Os X Server	10.3.3	All	All	All
Operating System	Apple	Mac Os X Server	10.3.4	All	All	All
Operating System	Apple	Mac Os X Server	10.3.5	All	All	All
Operating System	Apple	Mac Os X Server	10.3.6	All	All	All
Operating System	Apple	Mac Os X Server	10.3.7	All	All	All
Operating System	Apple	Mac Os X Server	10.3.8	All	All	All
Operating System	Apple	Mac Os X Server	10.3.9	All	All	All
Operating System	Apple	Mac Os X Server	10.4	All	All	All
Operating	Apple	Mac Os X Server	10.4.1	All	All	All


```

vpc2.vpc.amazonaws.com_v3_1.0.0. . . . .

```

```
cpe:2.3:o:apple:mac_os_x:10.3.1:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.3:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.4:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.5:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.6:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.7:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.8:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x:10.3.9:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4.1:*.:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4.2:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4.5:*.:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4.6:*.:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.1:*.:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.2:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.3:*.:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.5:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.6:*.:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.7:*.:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.8:*.:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.3.9:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4.1:*.:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4.2:*.:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.4.4:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x:10.4.5:*.:.:.:.:.:
```

```
cpe:2.3:o:apple:mac os x:10.4.6:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x server:10.3:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x_server:10.3.1:::*:*:*:*.*
```

```
cpe:2.3:o:apple:mac os x server:10.3.2:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x server:10.3.3:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x server:10.3.4:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x server:10.3.5:*:*:*:*:*.*
```

```
cpe:2.3:o:apple:mac_os_x_server:10.3.6:::*:*:*:*.*
```

```
cpe:2.3:o:apple:mac_os_x_server:10.3.7:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x server:10.3.8:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x server:10.3.9:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x_server:10.4:*:*:*:*:*:*
```

```
cpe:2.3:o:apple:mac_os_x_server:10.4.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x server:10.4.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x server:10.4.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x_server:10.4.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x server:10.4.5:*.:*:*:*:*.*
```

```
cpe:2.3:o:apple:mac_os_x_server:10.4.6:*.:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x_server:10.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x_server:10.3.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x_server:10.3.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x server:10.3.3:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x_server:10.3.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x_server:10.3.5:*:*:*:*:*:*:
```

cpe:2.3:o:apple:mac_os_x_server:10.3.6:*****:
cpe:2.3:o:apple:mac_os_x_server:10.3.7:*****:
cpe:2.3:o:apple:mac_os_x_server:10.3.8:*****:
cpe:2.3:o:apple:mac_os_x_server:10.3.9:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.1:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.2:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.3:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.4:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.5:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.6:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)