



CVE-2002-0655

Published on: 07/31/2002 12:00:00 AM UTC

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

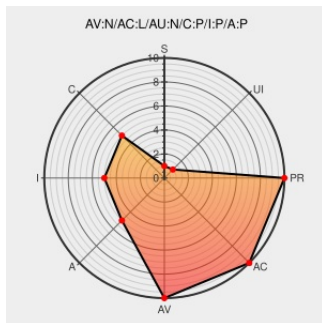
CVE-2002-0655

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

OpenSSL 0.9.6d and earlier, and 0.9.7-beta2 and earlier, does not properly handle ASCII representations of integers on 64 bit platforms, which could allow attackers to cause a denial of service and possibly execute arbitrary code.

CVE-2002-0655 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

<ftp.freebsd.org>

[text/plain](#)

[Inactive Link](#) **Not Archived**

[FREEBSD FreeBSD-SA-02:33](#)

No Description Provided

<ftp.caldera.com>

[Inactive Link](#) **Not Archived**

[CALDERA CSSA-2002-033.1](#)

CERT Advisory CA-2002-23 Multiple Vulnerabilities In OpenSSL

[US Government Resource](#)

www.cert.org

[text/html](#)

[CERT CA-2002-23](#)

Home - Conectiva

distro.conectiva.com.br

[text/html](#)

[CONECTIVA CLA-2002:513](#)

No Description Provided

www.linux-mandrake.com

[MANDRAKE MDKSA-2002:046](#)

Inactive Link Not Archived

CERT/CC Vulnerability Note VU#308891

US Government Resource

www.kb.cert.org

text/html

CERT-VN VU#308891

No Description Provided

ftp.caldera.com

CALDERA CSSA-2002-033.0

Inactive Link Not Archived

OpenSSL ASCII Representation Of Integers Buffer Overflow Vulnerability

cve.report (archive)

text/html

BID 5364

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	Apple	Mac Os X	10.0	All	All	All
Operating System	Apple	Mac Os X	10.0.1	All	All	All
Operating System	Apple	Mac Os X	10.0.2	All	All	All
Operating System	Apple	Mac Os X	10.0.3	All	All	All
Operating System	Apple	Mac Os X	10.0.4	All	All	All
Operating System	Apple	Mac Os X	10.1	All	All	All
Operating System	Apple	Mac Os X	10.1.1	All	All	All
Operating System	Apple	Mac Os X	10.1.2	All	All	All
Operating System	Apple	Mac Os X	10.1.3	All	All	All
Operating System	Apple	Mac Os X	10.1.4	All	All	All
Operating System	Apple	Mac Os X	10.1.5	All	All	All
Operating System	Apple	Mac Os X	10.0	All	All	All
Operating System	Apple	Mac Os X	10.0.1	All	All	All
Operating System	Apple	Mac Os X	10.0.2	All	All	All

System						
Operating System	Apple	Mac Os X	10.0.3	All	All	All
Operating System	Apple	Mac Os X	10.0.4	All	All	All
Operating System	Apple	Mac Os X	10.1	All	All	All
Operating System	Apple	Mac Os X	10.1.1	All	All	All
Operating System	Apple	Mac Os X	10.1.2	All	All	All
Operating System	Apple	Mac Os X	10.1.3	All	All	All
Operating System	Apple	Mac Os X	10.1.4	All	All	All
Operating System	Apple	Mac Os X	10.1.5	All	All	All
Application	Openssl	Openssl	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6b	All	All	All
Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6b	All	All	All
Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All

Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Oracle	Application Server	All	All	All	All
Application	Oracle	Application Server	1.0.2	All	All	All
Application	Oracle	Application Server	1.0.2.1s	All	All	All
Application	Oracle	Application Server	1.0.2.2	All	All	All
Application	Oracle	Application Server	All	All	All	All
Application	Oracle	Application Server	1.0.2	All	All	All
Application	Oracle	Application Server	1.0.2.1s	All	All	All
Application	Oracle	Application Server	1.0.2.2	All	All	All
Application	Oracle	Corporate Time Outlook Connector	3.1	All	All	All
Application	Oracle	Corporate Time Outlook Connector	3.1.1	All	All	All
Application	Oracle	Corporate Time Outlook Connector	3.1.2	All	All	All
Application	Oracle	Corporate Time Outlook Connector	3.3	All	All	All
Application	Oracle	Corporate Time Outlook Connector	3.1	All	All	All
Application	Oracle	Corporate Time Outlook Connector	3.1.1	All	All	All
Application	Oracle	Corporate Time Outlook Connector	3.1.2	All	All	All
Application	Oracle	Corporate Time Outlook Connector	3.3	All	All	All
Application	Oracle	Http Server	9.0.1	All	All	All
Application	Oracle	Http Server	9.2.0	All	All	All
Application	Oracle	Http Server	9.0.1	All	All	All
Application	Oracle	Http Server	9.2.0	All	All	All
cpe:2.3:o:apple:mac_os_x:10.0:*****:						
cpe:2.3:o:apple:mac_os_x:10.0.1:*****:						
cpe:2.3:o:apple:mac_os_x:10.0.2:*****:						
cpe:2.3:o:apple:mac_os_x:10.0.3:*****:						
cpe:2.3:o:apple:mac_os_x:10.0.4:*****:						
cpe:2.3:o:apple:mac_os_x:10.1:*****:						
cpe:2.3:o:apple:mac_os_x:10.1.1:*****:						
cpe:2.3:o:apple:mac_os_x:10.1.2:*****:						
cpe:2.3:o:apple:mac_os_x:10.1.3:*****:						

```
cpe:2.3:o:apple:mac_os_x:10.14:*:*:*:*:*:*
```

```
cpe:2.3:o:apple:mac_os_x:10.1.5:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.0.1:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.0.2:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.0.3:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.0.4:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.1.1:::*:*:*:*:
```

```
cpe:2.3:o:apple:mac os x:10.1.2:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.1.3:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.1.4:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os_x:10.1.5:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.1c:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.2b:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.5a:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.6:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.6a:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.6b:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.6c:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.6d:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.7:beta1:*.:*:*:*:*:
```

cpe:2.3:a:openssl:openssl:0.9.7:beta2:*:*:*:*:*:

```
cpe:2.3:a:openssl:openssl:0.9.1c:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.2b:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.5a:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.6:.*:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:openssl:openssl:0.9.6a:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.6b:*:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.6c:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.6d:*:*:*:*:*:
```

```
cpe:2.3:a:openssl:openssl:0.9.7:beta1:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:openssl:openssl:0.9.7:beta2:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:application_server:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:application_server:1.0.2:*:*:*:*:*:*
```

```
cpe:2.3:a:oracle:application_server:1.0.2.1s:*.:.:*.:.:*.:.:*
```

```
cpe:2.3:a:oracle:application_server:1.0.2.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:application_server:*.:.:.:.:.:.:
```

```
cpe:2.3:a:oracle:application_server:1.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:application_server:1.0.2.1s:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:oracle:application_server:1.0.2.2:*:*:*:*:*.*
```

cpe:2.3:a:oracle:corporate_time_outlook_connector:3.1:*:*:*:*:*:

cpe:2.3:a:oracle:corporate_time_outlook_connector:3.1.1:*:*:*:*:*:

cpe:2.3:a:oracle:corporate_time_outlook_connector:3.1.2:*:*:*:*:*:

cpe:2.3:a:oracle:corporate_time_outlook_connector:3.3:*:*:*:*:*:

cpe:2.3:a:oracle:corporate_time_outlook_connector:3.1:*:*:*:*:*:

cpe:2.3:a:oracle:corporate_time_outlook_connector:3.1.1:*:*:*:*:*:

cpe:2.3:a:oracle:corporate_time_outlook_connector:3.1.2:*:*:*:*:*:

cpe:2.3:a:oracle:corporate_time_outlook_connector:3.3:*:*:*:*:*.*

```
cpe:2.3:a:oracle:http_server:9.0.1:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:http_server:9.2.0:*:*:*:*:*:
```

cpe:2.3:a:oracle:http_server:9.0.1:*****:

cpe:2.3:a:oracle:http_server:9.2.0:*****:

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](#)