



CVE-2013-1618

Published on: 02/08/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:32 PM UTC

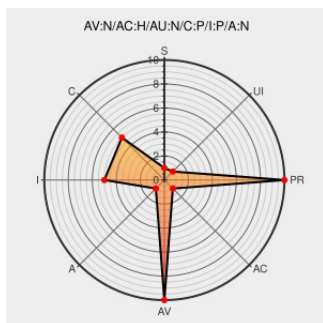
CVE-2013-1618

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Opera Browser](#) from [Opera](#) contain the following vulnerability:

The TLS implementation in Opera before 12.13 does not properly consider timing side-channel attacks on a MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, a related issue to CVE-2013-0169.

CVE-2013-1618 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

HIGH

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

NONE

CVE References

Description

Tags

Link

Opera 12.13 changelog

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

CONFIRM
www.opera.com/docs/changelogs/unified/1213/

Advisory: TLS response timings can indicate network contents - Opera Software

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

CONFIRM www.opera.com/support/kb/view/1044/

openSUSE-SU-2013:0289-1: moderate: Opera update to 12.14 version

[lists.opensuse.org](#)
[text/html](#)

SUSE [openSUSE-SU-2013:0289](#)

oss-security - Re: CVE request: TLS CBC padding timing flaw in various SSL / TLS implementations

[openwall.com](#)
[text/html](#)

MLIST [oss-security] 20130205 Re: CVE request: TLS CBC padding timing flaw in various SSL / TLS implementations

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
Application	Opera	Opera Browser	12.00	All	All	All
Application	Opera	Opera Browser	12.00	beta	All	All
Application	Opera	Opera Browser	12.01	All	All	All
Application	Opera	Opera Browser	12.02	All	All	All
Application	Opera	Opera Browser	12.10	All	All	All
Application	Opera	Opera Browser	12.10	beta	All	All
Application	Opera	Opera Browser	12.11	All	All	All
Application	Opera	Opera Browser	12.00	All	All	All
Application	Opera	Opera Browser	12.00	beta	All	All
Application	Opera	Opera Browser	12.01	All	All	All
Application	Opera	Opera Browser	12.02	All	All	All
Application	Opera	Opera Browser	12.10	All	All	All
Application	Opera	Opera Browser	12.10	beta	All	All
Application	Opera	Opera Browser	12.11	All	All	All
Application	Opera	Opera Browser	All	All	All	All

cpe:2.3:a:opera:opera_browser:12.00:*****:.*:

cpe:2.3:a:opera:opera_browser:12.00:beta:*****:.*:

cpe:2.3:a:opera:opera_browser:12.01:*****:.*:

cpe:2.3:a:opera:opera_browser:12.02:*****:.*:

cpe:2.3:a:opera:opera_browser:12.10:*****:.*:

cpe:2.3:a:opera:opera_browser:12.10:beta:*****:.*:

cpe:2.3:a:opera:opera_browser:12.11:*****:.*:

cpe:2.3:a:opera:opera_browser:12.00:*****:.*:

cpe:2.3:a:opera:opera_browser:12.00:beta:*****:.*:

cpe:2.3:a:opera:opera_browser:12.01.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.02.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10:beta.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.11.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:*.*.*.*.*.*.*.

cpe:2.3:a:opera:opera_browser:12.01.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.02.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10:beta.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.11.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:*.*.*.*.*.*.*.

cpe:2.3:a:opera:opera_browser:12.01.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.02.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10:beta.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.11.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:*.*.*.*.*.*.*.

cpe:2.3:a:opera:opera_browser:12.01.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.02.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10:beta.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.11.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:*.*.*.*.*.*.*.

cpe:2.3:a:opera:opera_browser:12.01.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.02.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10:beta.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.11.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:*.*.*.*.*.*.*.

cpe:2.3:a:opera:opera_browser:12.01.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.02.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.10:beta.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:12.11.*.*.*.*.*.*.
cpe:2.3:a:opera:opera_browser:*.*.*.*.*.*.*.

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