



CVE-2008-7128

Published on: 08/31/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:15 PM UTC

CVE-2008-7128

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

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

The `ssl_parse_client_key_exchange` function in XySSL before 0.9 does not protect against certain Bleichenbacher attacks using chosen ciphertext, which allows remote attackers to recover keys via unspecified vectors.

CVE-2008-7128 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

SSL Library mbed TLS / PolarSSL

[polarssl.org](#)
[text/html](#)

[CONFIRM polarssl.org/?archive#001c](#)

IBM X-Force Exchange

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

[XF xyssl-sslparseclient-security-bypass\(41253\)](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

[VUPEN ADV-2008-0917](#)

By selecting these links, you may be leaving CVEreport workspace. 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.

cpe:2.3:a:xyssl:xyssl:0.6:*****:

cpe:2.3:a:xyssl:xyssl:0.7:*****:

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](#)