



# CVE-2017-3730

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2017-3730
<b>State</b>	PUBLIC
<b>Assigner</b>	openssl-security@openssl.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-05-04 19:29:00 UTC
<b>Updated</b>	2019-04-25 13:59:00 UTC
<b>Description</b>	In OpenSSL 1.1.0 before 1.1.0d, if a malicious server supplies bad parameters for a DHE or ECDHE key exchange then thi

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.1.0c	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Agile Engineering Data Management</a>	6.1.3	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Agile Engineering Data Management</a>	6.2.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Agile Engineering Data Management</a>	6.1.3	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Agile Engineering Data Management</a>	6.2.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Application Session Controller</a>	3.7.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Application Session Controller</a>	3.8.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Application Session Controller</a>	3.7.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Application Session Controller</a>	3.8.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Eagle Lnp Application Processor</a>	10.0	All	All	All

Application	Oracle	Communications Eagle Lnp Application Processor	10.1	All	All	All
Application	Oracle	Communications Eagle Lnp Application Processor	10.2	All	All	All
Application	Oracle	Communications Eagle Lnp Application Processor	10.0	All	All	All
Application	Oracle	Communications Eagle Lnp Application Processor	10.1	All	All	All
Application	Oracle	Communications Eagle Lnp Application Processor	10.2	All	All	All
Application	Oracle	Communications Operations Monitor	3.4	All	All	All
Application	Oracle	Communications Operations Monitor	4.0	All	All	All
Application	Oracle	Communications Operations Monitor	3.4	All	All	All
Application	Oracle	Communications Operations Monitor	4.0	All	All	All
Application	Oracle	Jd Edwards Enterpriseone Tools	9.2	All	All	All
Application	Oracle	Jd Edwards Enterpriseone Tools	9.2	All	All	All
Application	Oracle	Jd Edwards World Security	a9.1	All	All	All
Application	Oracle	Jd Edwards World Security	a9.2	All	All	All
Application	Oracle	Jd Edwards World Security	a9.3	All	All	All
Application	Oracle	Jd Edwards World Security	a9.4	All	All	All
Application	Oracle	Jd Edwards World Security	a9.1	All	All	All
Application	Oracle	Jd Edwards World Security	a9.2	All	All	All
Application	Oracle	Jd Edwards World Security	a9.3	All	All	All
Application	Oracle	Jd Edwards World Security	a9.4	All	All	All

## References

Reference	Source	Link
OpenSSL: Multiple vulnerabilities (GLSA 201702-07) — Gentoo Security	GENTOO	<a href="#">sec</a>
Fix missing NULL checks in CKE processing · openssl/openssl@efbe126 · GitHub	MISC	<a href="#">git</a>
<a href="http://www.openssl.org/news/secadv/20170126.txt">www.openssl.org/news/secadv/20170126.txt</a>	CONFIRM	<a href="#">ww</a>
Oracle Critical Patch Update - January 2018	CONFIRM	<a href="#">ww</a>
OpenSSL Multiple Bugs Let Remote Users Deny Service and Obtain Potentially Sensitive Information - SecurityTracker	SECTRACK	<a href="#">ww</a>
OpenSSL 1.1.0 - Remote Client Denial of Service - Multiple dos Exploit	EXPLOIT-DB	<a href="#">ww</a>
OpenSSL CVE-2017-3730 NULL Pointer Dereference Denial of Service Vulnerability	BID	<a href="#">ww</a>
Document Display   HPE Support Center	CONFIRM	<a href="#">sup</a>
Oracle Critical Patch Update - October 2017	CONFIRM	<a href="#">ww</a>
Oracle Critical Patch Update Advisory - April 2019	MISC	<a href="#">ww</a>
CVE Program record	CVE.ORG	<a href="#">ww</a>
NVD vulnerability detail	NVD	<a href="#">nvc</a>

Discovery Credit

**LEGACY:** Guido Vranken

#### Legacy QID Mappings

[43835](#) HPE Switches And Routers Open Secure Sockets Layer (OpenSSL) Multiple Remote Vulnerabilities (HPESBHF03838)

© [CVE.report](#) 2026 |

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](#)