



# Encrypt-Then-Mac renegotiation crash

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

## Summary

<b>CVE</b>	CVE-2017-3733
<b>State</b>	PUBLISHED
<b>Assigner</b>	openssl
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-05-04 19:29:00 UTC
<b>Updated</b>	2025-04-20 01:37:25 UTC
<b>Description</b>	During a renegotiation handshake if the Encrypt-Then-Mac extension is negotiated where it was not in the original handsha

## Risk And Classification

**Primary CVSS:** v3.0 7.5 HIGH from nvd@nist.gov

**CVSS:**3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**Problem Types:** CWE-20 | protocol error

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:N/A:P

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Operations Agent	11.14	All	All	All
Application	Hp	Operations Agent	11.15	All	All	All
Application	Openssl	Openssl	1.1.0	All	All	All
Application	Openssl	Openssl	1.1.0a	All	All	All
Application	Openssl	Openssl	1.1.0b	All	All	All
Application	Openssl	Openssl	1.1.0c	All	All	All
Application	Openssl	Openssl	1.1.0d	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenSSL	OpenSSL	affected openssl-1.1.0	Not specified
CNA	OpenSSL	OpenSSL	affected openssl-1.1.0a	Not specified
CNA	OpenSSL	OpenSSL	affected openssl-1.1.0b	Not specified
CNA	OpenSSL	OpenSSL	affected openssl-1.1.0c	Not specified
CNA	OpenSSL	OpenSSL	affected openssl-1.1.0d	Not specified

### References

Reference

OpenSSL CVE-2017-3733 Denial of Service Vulnerability

OpenSSL Flaw in Encrypt-Then-Mac Extension Negotiation Lets Remote Authenticated Users Cause the Target Service to Crash - SecurityTr

Don't change the state of the ETM flags until CCS processing · openssl/openssl@4ad9361 · GitHub

www.openssl.org/news/secadv/20170216.txt

Oracle Critical Patch Update - October 2017

Oracle Critical Patch Update - January 2018

Document Display | HPE Support Center

Oracle Critical Patch Update Advisory - April 2019

CVE Program record

NVD vulnerability detail



### Vendor Comments And Credit

Discovery Credit

**CNA:** Joe Orton (Red Hat) (en)

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)