



CVE-2019-0190

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-0190
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-30 22:29:00 UTC
Updated	2023-11-07 03:01:00 UTC
Description	A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.4.37	All	All	All
Application	Apache	Http Server	2.4.37	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.3.3	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.3.3	All	All	All
Application	Oracle	Hospitality Guest Access	4.2.0	All	All	All
Application	Oracle	Hospitality Guest Access	4.2.1	All	All	All
Application	Oracle	Hospitality Guest Access	4.2.0	All	All	All
Application	Oracle	Hospitality Guest Access	4.2.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.2	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.3	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.2	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.3	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.0	All	All	All

Application	Oracle	Retail Xstore Point Of Service	7.1	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.1	All	All	All

References

Reference	Source	Link	Tags
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	Mail
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	Mail
Oracle Critical Patch Update Advisory - July 2021	N/A	www.oracle.com	
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	Mail
January 2019 Apache HTTP Server Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	Trust
Pony Mail!	MLIST	lists.apache.org	
Apache: Multiple vulnerabilities (GLSA 201903-21) — Gentoo security	GENTOO	security.gentoo.org	Trust
Pony Mail!		lists.apache.org	
Oracle Critical Patch Update - July 2019	MISC	www.oracle.com	Trust
Apache HTTP Server CVE-2019-0190 Denial of Service Vulnerability	BID	www.securityfocus.com	Trust
Pony Mail!	MLIST	lists.apache.org	
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	CONFIRM	httpd.apache.org	Verified
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	

Pony Mail!	MLIS I	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	Mi
Oracle Critical Patch Update Advisory - April 2019	MISC	www.oracle.com	Tr
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[377378](#) Alibaba Cloud Linux Security Update for httpd:2.4 (ALINUX3-SA-2022:0017)

[500016](#) Alpine Linux Security Update for apache2

[503707](#) Alpine Linux Security Update for apache2

[710186](#) Gentoo Linux Apache Multiple vulnerabilities (GLSA 201903-21)

© [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](#)