



# CVE-2017-9788

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

## Summary

<b>CVE</b>	CVE-2017-9788
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-07-13 16:29:00 UTC
<b>Updated</b>	2023-11-07 02:50:00 UTC
<b>Description</b>	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest'

## Risk And Classification

**Problem Types:** CWE-200 | CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Application	Apache	Http Server	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Oracle	Secure Global Desktop	5.3	All	All	All
Application	Oracle	Secure Global Desktop	5.3	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All



Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Jboss Core Services	1.0	All	All	All
Application	Redhat	Jboss Core Services	1.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.4.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.4.0	All	All	All
Application	Redhat	Jboss Enterprise Web Server	2.0.0	All	All	All
Application	Redhat	Jboss Enterprise Web Server	2.0.0	All	All	All

## References

### Reference

Red Hat Customer Portal

Pony Mail!

July 2017 Apache httpd Server Vulnerabilities in Multiple NetApp Products | NetApp Product Security

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Document Display | HPE Support Center

About the security content of macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan - Apple

Pony Mail!

Pony Mail!

Pony Mail!


Red Hat Customer Portal

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat Customer Portal
Red Hat Customer Portal
Pony Mail!
Apache mod_auth_digest Uninitialized Memory Error Lets Remote Users Obtain Potentially Sensitive Information and Deny Service - Security
Pony Mail!
Pony Mail!
[R1] Tenable.sc 5.13.0 Fixes Multiple Third-Party Vulnerabilities - Security Advisory   Tenable®
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
httpd 2.2 vulnerabilities - The Apache HTTP Server Project
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!

Pony Mail!
Apache: Multiple vulnerabilities (GLSA 201710-32) — Gentoo security
Pony Mail!
Apache HTTP Server CVE-2017-9788 Memory Corruption Vulnerability
Pony Mail!
Pony Mail!
Oracle Critical Patch Update - October 2017
Debian -- Security Information -- DSA-3913-1 apache2
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.
<b>Legacy QID Mappings</b>
378141 Virtuozzo Linux Security Update for mod_ssl (VZLSA-2017:2478)

© 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](#)**