



Common Vulnerabilities and Exposures

[CVE List](#)[About](#)[CNAs](#)[Board](#)
[News & Blog](#)**NVD**

Go to for:

[CVSS Scores](#)
[CPE Info](#)
[Advanced Search](#)[Full-Screen View](#)

CVE-ID	
CVE-2018-1312	Learn more at National Vulnerability Database (NVD). • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent replay attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MLIST:[oss-security] 20180323 CVE-2018-1312: Weak Digest auth nonce generation in mod_auth_digest • URL:http://www.openwall.com/lists/oss-security/2018/03/24/7 • MLIST:[debian-lts-announce] 20180530 [SECURITY] [DLA 1389-1] apache2 security update • URL:https://lists.debian.org/debian-lts-announce/2018/05/msg00020.html • CONFIRM:https://httpd.apache.org/security/vulnerabilities_24.html • CONFIRM:https://security.netapp.com/advisory/ntap-20180601-0004/ • DEBIAN:DSA-4164 • URL:https://www.debian.org/security/2018/dsa-4164 • REDHAT:RHSA-2018:3558 • URL:https://access.redhat.com/errata/RHSA-2018:3558 • UBUNTU:USN-3627-1 • URL:https://usn.ubuntu.com/3627-1/ • UBUNTU:USN-3627-2 • URL:https://usn.ubuntu.com/3627-2/ • BID:103524 • URL:http://www.securityfocus.com/bid/103524 • SECTrack:1040571 • URL:http://www.securitytracker.com/id/1040571	
Assigning CNA	
Apache Software Foundation	WIZ, Inc. EXHIBIT - 1102 WIZ, Inc. v. Orca Security LTD.

Date Entry Created	
20171207	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20171207)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is an entry on the CVE List , which provides common identifiers for publicly known cybersecurity vulnerabilities.	
SEARCH CVE USING KEYWORDS: Submit	
You can also search by reference using the CVE Reference Maps .	
For More Information: cve@mitre.org	