



CVE-2016-0701

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

Summary

CVE	CVE-2016-0701
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-02-15 02:59:00 UTC
Updated	2023-02-12 23:15:00 UTC
Description	The DH_check_pub_key function in crypto/dh/dh_check.c in OpenSSL 1.0.2 before 1.0.2f does not ensure that prime num

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2e	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All

Application	Openssl	Openssl	1.0.2e	All	All	All
-------------	---------	---------	--------	-----	-----	-----

References

Reference

Document Display | HPE Support Center

www.openssl.org/news/secadv/20160128.txt

[security-announce] openSUSE-SU-2016:0637-1: important: Security update

OpenSSL Flaws Let Remote Users Recover DH Keys in Certain Cases and Let Remote Users Negotiate Disabled Ciphers - SecurityTracker

Oracle Critical Patch Update - July 2016

Oracle July 2016 Critical Patch Update Multiple Vulnerabilities

USN-2883-1: OpenSSL vulnerability | Ubuntu

OpenSSL: Multiple vulnerabilities (GLSA 201601-05) — Gentoo security

Oracle Critical Patch Update Advisory - July 2020

git.openssl.org Git - openssl.git/commit

git.openssl.org Git - openssl.git/commit

Oracle Critical Patch Update Advisory - October 2020

OpenSSL CVE-2016-0701 Security Bypass Vulnerability

Vulnerability Note VU#257823 - OpenSSL re-uses unsafe prime numbers in Diffie-Hellman protocol

Document Display | HPE Support Center

Oracle Critical Patch Update - July 2019

git.openssl.org Git - openssl.git/commit

cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf

Document Display | HPE Support Center

[SECURITY] Fedora 23 Update: openssl-1.0.2f-1.fc23

git.openssl.org Git - openssl.git/commit

Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates

Into the symmetry: OpenSSL Key Recovery Attack on DH small subgroups (CVE-2016-0701)

Oracle Critical Patch Update Advisory - January 2020

Oracle Critical Patch Update Advisory - April 2020

Oracle Critical Patch Update - October 2017

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

591280 Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)

© [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](#)