NVD MENU

NATIONAL VULNERABILITY DATABASE

NATIONAL VULNERABILITY DATABASE
NVD

VULNERABILITIES

CVE-2023-2283 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

A vulnerability was found in libssh, where the authentication check of the connecting client can be bypassed i the`pki_verify_data_signature` function in memory allocation problems. This issue may happen if there is insufficient memory or the memory usage is limited. The problem is caused by the return value `rc,` which is initialized to SSH_ERROR and later rewritten to save the return value of the function call `pki_key_check_hash_compatible.` The value of the variable is not changed between this point and the cryptographic verification. Therefore any error between them calls `goto error` returning SSH_OK.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** **6.5 MEDIUM**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://packetstormsecurity.com/files/172861/libssh-0.9.6-0.10.4-pki_verify_data_signature-Authorization-Bypass.html	
https://access.redhat.com/security/cve/CVE-2023-2283	Third Party Advisory
https://bugzilla.redhat.com/show_bug.cgi?id=2189736	Issue Tracking Third Party Advisory
https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/27PD44ALQTZXX7K6JAM3BXBUHYA6DFFN/	
https://security.gentoo.org/glsa/202312-05	
https://security.netapp.com/advisory/ntap-20240201-0005/	
https://www.libssh.org/security/advisories/CVE-2023-2283.txt	Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-287	Improper Authentication	NIST Red Hat, Inc.

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

□ **cpe:2.3:a:libssh:libssh:*:*:*:*:*:*:*:*** Show Matching CPE(s)□	**From (including)** **0.9.1**	**Up to (including)** **0.9.6**
□ **cpe:2.3:a:libssh:libssh:*:*:*:*:*:*:*:*** Show Matching CPE(s)□	**From (including)** **0.10.0**	**Up to (including)** **0.10.4**

Configuration 2 (hide)

□ **cpe:2.3:o:fedoraproject:fedora:37:*:*:*:*:*:*:***

Show Matching CPE(s)□

Configuration 3 (hide)

□ **cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:***

Show Matching CPE(s)□

□ **cpe:2.3:o:redhat:enterprise_linux:9.0:*:*:*:*:*:*:***

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899
(301) 975-2000

Webmaster | Contact Us | Our Other Offices

Incident Response Assistance and Non-NVD Related
Technical Cyber Security Questions:
US-CERT Security Operations Center
Email: soc@us-cert.gov
Phone: 1-888-282-0870

Site Privacy | Accessibility | Privacy Program | Copyrights | Vulnerability Disclosure | No Fear Act Policy | FOIA | Environmental Policy | Scientific Integrity | Information Quality Standards | Commerce.gov | Science.gov | USA.gov