CVE-2018-15473

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-15473
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-17 19:29:00 UTC
Updated	2023-02-23 23:13:00 UTC
Description	OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating u

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	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	Aff Baseboard Management Controller	-	All	All	All
Application	Netapp	Aff Baseboard Management Controller	-	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Operating System	Netapp	Clustered Data Ontap	-	All	All	All
Operating System	Netapp	Clustered Data Ontap	-	All	All	All
Operating System	Netapp	Clustered Data Ontap	-	All	All	All

Operating System	Netapp	Clustered Data Ontap	-	All	All	All
Hardware	Netapp	Cn1610	-	All	All	All
Hardware	Netapp	Cn1610	-	All	All	All
Operating System	Netapp	Cn1610 Firmware	-	All	All	All
Operating System	Netapp	Cn1610 Firmware	-	All	All	All
Operating System	Netapp	Data Ontap	-	All	All	All
Operating System	Netapp	Data Ontap	-	All	All	All
Application	Netapp	Data Ontap Edge	-	All	All	All
Application	Netapp	Data Ontap Edge	-	All	All	All
Application	Netapp	Fas Baseboard Management Controller	-	All	All	All
Application	Netapp	Fas Baseboard Management Controller	-	All	All	All
Application	Netapp	Oncommand Unified Manager	All	All	All	All
Application	Netapp	Oncommand Unified Manager	All	All	All	All
Application	Netapp	Ontap Select Deploy	-	All	All	All
Application	Netapp	Ontap Select Deploy	-	All	All	All
Application	Netapp	Service Processor	-	All	All	All
Application	Netapp	Service Processor	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Application	Netapp	Storage Replication Adapter	All	All	All	All
Application	Netapp	Storage Replication Adapter	All	All	All	All
Application	Netapp	Vasa Provider	All	All	All	All
Application	Netapp	Vasa Provider	All	All	All	All
Application	Netapp	Virtual Storage Console	All	All	All	All
Application	Netapp	Virtual Storage Console	All	All	All	All
Application	Openbsd	Openssh	All	All	All	All
Application	Oracle	Sun Zfs Storage Appliance Kit	8.8.6	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	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

Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Hardware	Siemens	Scalance X204rna	-	All	All	All
Operating System	Siemens	Scalance X204rna Firmware	All	All	All	All

References

Reference	Sou
Security Advisory	CON
oss-security - OpenSSH Username Enumeration	MIS
OpenSSH Authentication Attempt Processing Lets Remote Users Determine Valid Usernames on the Target System - SecurityTracker	SEC
OpenSSH 2.3 < 7.4 - Username Enumeration (PoC)	EXP
CVE-2018-15473 OpenSSH Username Enumeration Vulnerability in NetApp Products | NetApp Product Security	CON
OpenSSH < 7.7 - User Enumeration (2) - Linux remote Exploit	EXP
delay bailout for invalid authenticating user until after the packet · openbsd/src@779974d · GitHub	MIS
[SECURITY] [DLA-1474-1] openssh security update	MLI
#906236 - openssh: CVE-2018-15473: delay bailout for invalid authenticating user until after the packet - Debian Bug report logs	MIS
OpenSSH 2.3 < 7.7 - Username Enumeration	EXP
Debian -- Security Information -- DSA-4280-1 openssh	DEB
Red Hat Customer Portal	RED
Red Hat Customer Portal	RED
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CON
OpenSSH CVE-2018-15473 User Enumeration Vulnerability	BID
OpenSSH: User enumeration vulnerability (GLSA 201810-03) — Gentoo security	GEN
Oracle Critical Patch Update Advisory - January 2020	MIS
USN-3809-1: OpenSSH vulnerabilities | Ubuntu security notices	UBU
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296091 Oracle Solaris 11.4 Support Repository Update (SRU) 6.1.4 Missing (CPUJAN2019)

377465 Alibaba Cloud Linux Security Update for openssh (ALINUX2-SA-2019:0085)

378326 Virtuozzo Linux Security Update for openssh (VZLSA-2019:0711)

378878 Citrix XenServer Security Updates (CTX272237)

500486 Alpine Linux Security Update for openssh

504245 Alpine Linux Security Update for openssh

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

751241 OpenSUSE Security Update for ssh-audit (openSUSE-SU-2021:1383-1)