CVE-2018-1000805

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-1000805
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-08 15:29:00 UTC
Updated	2022-04-06 18:35:00 UTC
Description	Paramiko version 2.4.1, 2.3.2, 2.2.3, 2.1.5, 2.0.8, 1.18.5, 1.17.6 contains a Incorrect Access Control vulnerability in SSH se

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	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	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	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	Canonical	Ubuntu Linux	18.10	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
Application	Paramiko	Paramiko	1.17.6	All	All	All
Application	Paramiko	Paramiko	1.18.5	All	All	All
Application	Paramiko	Paramiko	2.0.8	All	All	All
Application	Paramiko	Paramiko	2.1.5	All	All	All

Application	Paramiko	Paramiko	2.2.3	All	All	All
Application	Paramiko	Paramiko	2.3.2	All	All	All
Application	Paramiko	Paramiko	2.4.1	All	All	All
Application	Paramiko	Paramiko	1.17.6	All	All	All
Application	Paramiko	Paramiko	1.18.5	All	All	All
Application	Paramiko	Paramiko	2.0.8	All	All	All
Application	Paramiko	Paramiko	2.1.5	All	All	All
Application	Paramiko	Paramiko	2.2.3	All	All	All
Application	Paramiko	Paramiko	2.3.2	All	All	All
Application	Paramiko	Paramiko	2.4.1	All	All	All
Application	Redhat	Ansible Tower	3.3	All	All	All
Application	Redhat	Ansible Tower	3.3	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 Desktop	7.0	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 Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	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	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Par
[CVE-2018-1000805] Server-side auth vulnerability · Issue #1283 · paramiko/paramiko · GitHub	CONFIRM	github.com	Patch, Th
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Par
USN-3796-2: Paramiko vulnerability | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Par
USN-3796-1: Paramiko vulnerability | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Par
herolab.usd.de/wp-content/uploads/sites/4/usd20180023.txt	MISC	herolab.usd.de	Exploit, T
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Par
USN-3796-3: Paramiko vulnerability | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Par
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Par
[SECURITY] [DLA 1556-1] paramiko security update	MLIST	lists.debian.org	Mailing L
[SECURITY] [DLA 2860-1] paramiko security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 178967 Debian Security Update for paramiko (DLA 2860-1)
- 378287 Virtuozzo Linux Security Update for python-paramiko (VZLSA-2018:3406)
- 500779 Alpine Linux Security Update for py3-paramiko
- 752721 SUSE Enterprise Linux Security Update for python-paramiko (SUSE-SU-2022:3730-1)
- 981117 Python (pip) Security Update for paramiko (GHSA-f2j6-wrhh-v25m)

CVE.report and Source URL Uptime Status status.cve.report