

Alpine Linux - Bug #10021

Bug # 10020 (Closed): py-paramiko: Authentication bypass in auth_handler.py (CVE-2018-1000805)

[3.8] py-paramiko: Authentication bypass in auth_handler.py (CVE-2018-1000805)

02/21/2019 11:39 AM - Alichia CH

Status: Closed	Start date: 02/21/2019
Priority: Normal	Due date:
Assignee:	% Done: 100%
Category: Security	Estimated time: 0.00 hour
Target version: 3.8.2	Security IDs: CVE-2018-1000805
Affected versions:	
Description Python Paramiko through versions 2.4.1, 2.3.2, 2.2.3, 2.1.5, 2.0.8, 1.18.5 and 1.17.6 is vulnerable to an authentication bypass in paramiko/auth_handler.py. A remote attacker could exploit this vulnerability in paramiko SSH servers to execute arbitrary code.	
Fixed In Version: python-paramiko 2.4.2, python-paramiko 2.3.3, python-paramiko 2.2.4, python-paramiko 2.1.6, python-paramiko 2.0.9	
References: https://github.com/paramiko/paramiko/issues/1283 https://nvd.nist.gov/vuln/detail/CVE-2018-1000805	
Patch: https://github.com/paramiko/paramiko/commit/56c96a65	

Associated revisions

Revision d6448b76 - 02/28/2019 02:29 PM - Leonardo Arena

main/py-paramiko: security upgrade to 2.4.2 (CVE-2018-1000805)

Fixes #10021

History

#1 - 02/28/2019 02:30 PM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset [alpine:d6448b760fceb43b000a3e57a4926509b5532d](https://git.alpinelinux.org/?id=alpine:d6448b760fceb43b000a3e57a4926509b5532d).

#2 - 03/05/2019 08:26 AM - Alichia CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed