CVE-2017-1000433

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-1000433
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-02 23:29:00 UTC
Updated	2021-03-04 21:16:00 UTC
Description	pysaml2 version 4.4.0 and older accept any password when run with python optimizations enabled. This allows attackers to

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	Pysaml2 Project	Pysaml2	All	All	All	All

References

Reference
PySAML2: Security bypass (GLSA 201801-11) — Gentoo security
[SECURITY] [DLA 2577-1] python-pysaml2 security update
[SECURITY] [DLA 1410-1] python-pysaml2 security update
Running python with optimizations makes UsernamePasswordMako accept any password for any user · Issue #451 · rohe/pysaml2 · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710314 Gentoo Linux PySAML2 Security bypass Vulnerability (GLSA 201801-11)

981178 Python (pip) Security Update for pysaml2 (GHSA-924m-4pmx-c67h)

Free CVE JSON API cve.report/api

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