



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)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)