



CVE-2011-1950

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2011-1950
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-06-06 19:55:00 UTC
Updated	2018-10-09 19:32:00 UTC
Description	plone.app.users in Plone 4.0 and 4.1 allows remote authenticated users to modify the properties of arbitrary accounts via ui

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Plone	Plone	4.0	All	All	All
Application	Plone	Plone	4.1	All	All	All
Application	Plone	Plone	4.0	All	All	All
Application	Plone	Plone	4.1	All	All	All

References

Reference
Plone Multiple Security Vulnerabilities
IBM X-Force Exchange
72729
About Secunia Research Flexera
SecurityFocus
Plone XSS and permission errors - SecurityReason.com
Security vulnerability announcement: CVE-2011-1950 – An escalation of privileges attack — Plone CMS: Open Source Content Management
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981405 Python (pip) Security Update for Plone (GHSA-2qx8-589j-gcpx)

© [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](#)