



CVE-2014-1927

Published on: 10/25/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:47 PM UTC

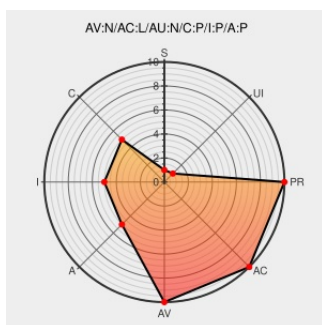
CVE-2014-1927

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Python-gnupg](#) from [Python-gnupg Project](#) contain the following vulnerability:

The `shell_quote` function in `python-gnupg 0.3.5` does not properly quote strings, which allows context-dependent attackers to execute arbitrary code via shell metacharacters in unspecified vectors, as demonstrated using `"$(` command-substitution sequences, a different vulnerability than CVE-2014-1928. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-7323.

CVE-2014-1927 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Security Advisory SA56616 - python-gnupg Command Injection Vulnerabilities - Secunia

[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 56616](#)

python-gnupg - Project Hosting on Google Code

[code.google.com](#)
[text/html](#)

[G](#) [CONFIRM](#)
[code.google.com/p/python-gnupg/](#)

oss-sec: Re: CVE request: python-gnupg before 0.3.5 shell injection

[Exploit](#)
[seclists.org](#)
[text/html](#)

[E](#) [MLIST \[oss-security\] 20140204](#)
Re: CVE request: python-gnupg
before 0.3.5 shell injection

Security Advisory SA59031 - Debian update for python-gnupg - Secunia

[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 59031](#)

Debian -- Security Information -- DSA-2946-1 python-gnupg

[www.debian.org](#)

[D](#) [DEBIAN DSA-2946](#)

Deprecated Link

text/html

oss-sec: Re: CVE request: python-gnupg before 0.3.5 shell injection

Exploit

seclists.org

text/html

 MLIST [oss-security] 20140209
Re: CVE request: python-gnupg
before 0.3.5 shell injection

Issue 98 - python-gnupg - Invalid security fix against shell injection - gnupg.py is
a Python API which wraps the GNU Privacy Guard. - Google Project Hosting

Exploit

code.google.com

text/html

 CONFIRM
code.google.com/p/python-
gnupg/issues/detail?id=98

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[980895](#) Python (pip) Security Update for python-gnupg (GHSA-r3vr-prvw-86g9)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Python-gnupg Project	Python-gnupg	0.3.5	All	All	All
Application	Python-gnupg Project	Python-gnupg	0.3.5	All	All	All
cpe:2.3:a:python-gnupg_project:python-gnupg:0.3.5:*:*:*:*:*:						
cpe:2.3:a:python-gnupg_project:python-gnupg:0.3.5:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

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