



CVE-2008-2942

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2008-2942
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-30 20:41:00 UTC
Updated	2018-10-11 20:45:00 UTC
Description	Directory traversal vulnerability in patch.py in Mercurial 1.0.1 allows user-assisted attackers to modify arbitrary files via ".." (

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mercurial	Mercurial	1.0.1	All	All	All
Application	Mercurial	Mercurial	1.0.1	All	All	All

References

Reference	Source	Link
wiki.rpath.com/Advisories:rPSA-2008-0211	CONFIRM	wiki.rpath.com
Gentoo update for mercurial - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Mercurial Multiple Vulnerabilities - Secunia.com	SECUNIA	secunia.com
oss-security - CVE id request mercurial:Insufficient input validation	MLIST	www.openwall.com
SecurityFocus	BUGTRAQ	www.securityfocus.com
[security-announce] SUSE Security Summary Report SUSE-SR:2008:015	SUSE	lists.opensuse.org
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
issues.rpath.com/browse/RPL-2633	CONFIRM	issues.rpath.com
Mercurial 'patch.py' Directory Traversal Vulnerability	BID	www.securityfocus.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud
Mercurial: 87c704ac92d4	CONFIRM	www.selenic.com
oss-security - Re: CVE id request mercurial:Insufficient input validation	MLIST	www.openwall.com

Mercurial: Directory traversal — Gentoo Linux Documentation	GENTOO	security.gentoo.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995369](#) Python (Pip) Security Update for mercurial (GHSA-v2gw-x5jf-pgww)

© [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](#).

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