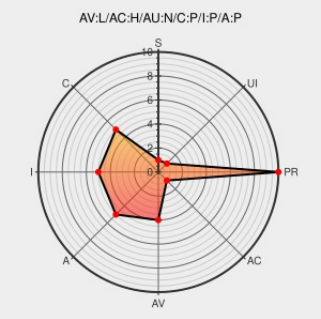
CVE-2005-1941

Published on: 06/08/2005 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1941

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Silvercity from Silvercity contain the following vulnerability:

SilverCity before 0.9.5-r1 installs (1) cgi-styler-form.py, (2) cgi-styler.py, and (3) source2html.py with read and write world permissions, which allows local users to execute arbitrary code.

CVE-2005-1941 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 3.7 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SilverCity File Permissions Let Local Users Gain Elevated Privileges - SecurityTracker	securitytracker.com, text/html	SECTRACK 1014153
Gentoo Linux Documentation -- SilverCity: Insecure file permissions	Patch, Vendor Advisory, www.gentoo.org, text/html	GENTOO GLSA-200506-05
Gentoo Bug 93558 - app-text/silvercity-0.9.5 contains world writable executables	Patch, Vendor Advisory, bugs.gentoo.org, text/html	MISC bugs.gentoo.org/show_bug.cgi?id=93558
Gentoo update for silvercity - Advisories - Secunia	web.archive.org, text/html	SECUNIA 15632

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Silvercity	Silvercity	0.9.5_r1	All	All	All
Application	Silvercity	Silvercity	0.9.5_r1	All	All	All

cpe:2.3:a:silvercity:silvercity:0.9.5_r1:*:*:*:*:*:*:*:

cpe:2.3:a:silvercity:silvercity:0.9.5_r1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→