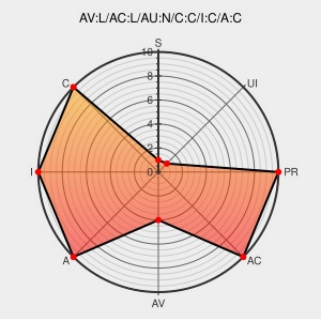
CVE-2005-1632

Published on: 05/17/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:25 PM UTC

CVE-2005-1632

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



Certain versions of Cheetah from Tavis Rudd contain the following vulnerability:

Cheetah 0.9.15 and 0.9.16 searches the /tmp directory for modules before using the paths in the PYTHONPATH variable, which allows local users to execute arbitrary code via a malicious module in /tmp/.

CVE-2005-1632 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Secunia - Advisories - Cheetah Insecure Module Importing Vulnerability	Vendor Advisory, web.archive.org, text/html	SECUNIA 15386
SourceForge.net: cheetahtemplate-discuss	Patch, sourceforge.net, application/octet-stream, Inactive Link, Not Archived	CONFIRM sourceforge.net/mailarchive/forum.php?thread_id=7070332&forum_id=1542
No Description Provided	www.osvdb.org, Inactive Link, Not Archived	OSVDB 16622

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

995315 Python (Pip) Security Update for cheetah (GHSA-vxf2-7rc3-pxmx)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tavis Rudd	Cheetah	0.9.15	All	All	All
Application	Tavis Rudd	Cheetah	0.9.16	All	All	All
Application	Tavis Rudd	Cheetah	0.9.15	All	All	All
Application	Tavis Rudd	Cheetah	0.9.16	All	All	All

cpe:2.3:a:tavis_rudd:cheetah:0.9.15:*:*:*:*:*:*:*:

cpe:2.3:a:tavis_rudd:cheetah:0.9.16:*:*:*:*:*:*:*:

cpe:2.3:a:tavis_rudd:cheetah:0.9.15:*:*:*:*:*:*:*:

cpe:2.3:a:tavis_rudd:cheetah:0.9.16:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→