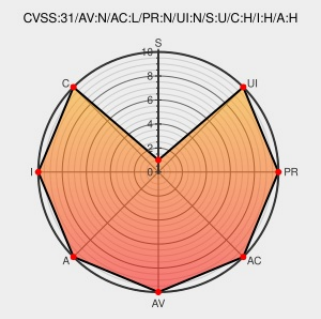
CVE-2014-4650

Published on: 02/20/2020 12:00:00 AM UTC

Last Modified on: 06/27/2022 04:20:00 PM UTC

CVE-2014-4650

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



Certain versions of Python from Python contain the following vulnerability:

The CGIHTTPServer module in Python 2.7.5 and 3.3.4 does not properly handle URLs in which URL encoding is used for path separators, which allows remote attackers to read script source code or conduct directory traversal attacks and execute unintended code via a crafted character sequence, as demonstrated by a %2f separator.

CVE-2014-4650 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
access.redhat.com | CVE-2014-4650	Third Party Advisory access.redhat.com text/html	REDHAT Red Hat

oss-security - Re: CVE ID Request for Python CGIHTTPServer File Disclosure	Mailing List Third Party Advisory openwall.com text/html	MISC openwall.com/lists/oss-security/2014/06/26/3
Issue 21766: CGIHTTPServer File Disclosure - Python tracker	Exploit Patch Vendor Advisory bugs.python.org text/html	MISC bugs.python.org/issue21766

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Python	Python	All	All	All	All
Application	Python	Python	2.7.5	All	All	All
Application	Python	Python	3.3.4	All	All	All
Application	Python	Python	2.7.5	All	All	All
Application	Python	Python	3.3.4	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Software Collections	-	All	All	All
Application	Redhat	Software Collections	-	All	All	All

cpe:2.3:a:python:python:*:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:2.7.5:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:2.7.5:*:*:*:*:*:*:*:

cpe:2.3:a:python:python:3.3.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:software_collections:-:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:software_collections:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→