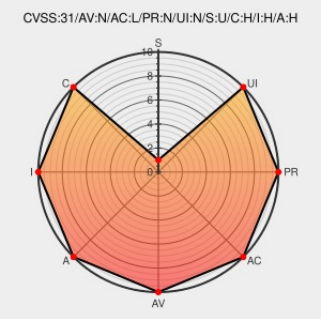
CVE-2017-1000158

Published on: 11/17/2017 12:00:00 AM UTC

Last Modified on: 02/16/2023 02:15:00 PM UTC

CVE-2017-1000158

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

CPython (aka Python) up to 2.7.13 is vulnerable to an integer overflow in the PyString_DecodeEscape function in stringobject.c, resulting in heap-based buffer overflow (and possible arbitrary code execution)

CVE-2017-1000158 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
CPython Integer Overflow in PyString_DecodeEscape() Lets Remote Users Execute Arbitrary Code - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1039890

[SECURITY] [DLA 1520-1] python3.4 security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180926 [SECURITY] [DLA 1520-1] python3.4 security update
Issue 30657: [security] CVE-2017-1000158: Unsafe arithmetic in PyString_DecodeEscape - Python tracker	Issue Tracking Patch Vendor Advisory bugs.python.org text/html	MISC bugs.python.org/issue30657
Python: Buffer overflow (GLSA 201805-02) — Gentoo Security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201805-02
CVE-2017-1000158 Python Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20230216-0001/
Debian -- Security Information -- DSA-4307-1 python3.5	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4307
[SECURITY] [DLA 1519-1] python2.7 security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180925 [SECURITY] [DLA 1519-1] python2.7 security update
[SECURITY] [DLA 1189-1] python2.7 security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20171124 [SECURITY] [DLA 1189-1] python2.7 security update
[SECURITY] [DLA 1190-1] python2.6 security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20171124 [SECURITY] [DLA 1190-1] python2.6 security update

Related QID Numbers

710291 Gentoo Linux Python Buffer overflow Vulnerability (GLSA 201805-02)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating	Debian	Debian Linux	8.0	All	All	All

System						
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All

- cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*
- cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*
- cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*
- cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*
- cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*
- cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*
- cpe:2.3:a:python:python:*:*:*:*:*:*:*:*
- cpe:2.3:a:python:python:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→