Bug 1901633 (CVE-2020-27783) - CVE-2020-27783 python-lxml: mXSS due to the use of improper parser

Keywords: Security ×

Status: CLOSED ERRATA
Alias: CVE-2020-27783
Product: Security Response
Component: vulnerability
Version: unspecified
Hardware: All
OS: Linux
Priority: medium
Severity: medium
Target Milestone: ---
Assignee: Red Hat Product Security
QA Contact:
Docs Contact:
URL:
Whiteboard:
Depends On: ~~1901634~~ 1902291 1902292 1902293 1902294 1903381 1910654 1969512
Blocks: 1896874
TreeView+ depends on / blocked

Reported: 2020-11-25 17:06 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-08-24 08:09 UTC (History)
CC List: 20 users (show)
Fixed In Version: lxml 4.6.2
Doc Type: If docs needed, set a value
Doc Text: A Cross-site Scripting (XSS) vulnerability was found in the python-lxml's clean module. The module's parser did not properly imitate browsers, causing different behaviors between the sanitizer and the user's page. This flaw allows a remote attacker to run arbitrary HTML/JS code. The highest threat from this vulnerability is to confidentiality and integrity.
Clone Of:
Environment:
Last Closed: 2021-05-18 14:36:52 UTC

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2021:3254	0	None	None	None	2021-08-24 08:08:59 UTC

Guilherme de Almeida Suckevicz 2020-11-25 17:06:43 UTC — Description

The python-lxml package from version 1.2 and before version 4.6.2 is vulnerable to mXSS due to the use of improper parser. The parser used doesn't imitate browsers, which causes different behaviours between the sanitizer and the user's page. This can result in an arbitrary HTML/JS code execution.

References:
https://pypi.org/project/lxml/4.6.1/
https://pypi.org/project/lxml/4.6.2/

Upstream patches:
https://github.com/lxml/lxml/commit/89e7aad6e7ff9ecd88678ff25f885988b184b26e
https://github.com/lxml/lxml/commit/a105ab8dc262ec6735977c25c13f0bdfcdec72a7

Guilherme de Almeida Suckevicz 2020-11-25 17:07:00 UTC — Comment 1

Created python-lxml tracking bugs for this issue:

Affects: fedora-all [~~bug 1901634~~]

Summer Long 2020-12-01 22:53:42 UTC — Comment 3

Upstream info for 4.6.2 fix:
https://github.com/lxml/lxml/commit/a105ab8dc262ec6735977c25c13f0bdfcdec72a7
https://pypi.org/project/lxml/4.6.2/

Salvatore Bonaccorso 2020-12-13 20:12:22 UTC — Comment 6

Hi

As the assigning CNA for CVE-2020-27783 can you clarify on the scope of it? Originally and by ~~https://bugzilla.redhat.com/show_bug.cgi?id=1901633#c0~~ this only seems to apply to https://github.com/lxml/lxml/commit/89e7aad6e7ff9ecd88678ff25f885988b184b26e which was fixed in 4.6.1 upstream. Later on upstream has referenced the CVE in the 4.6.2 notes but fixed there as well a second vector <math/svg> and <style> via in https://github.com/lxml/lxml/commit/a105ab8dc262ec6735977c25c13f0bdfcdec72a7 in 4.6.2.

Can you ideally assign a second CVE for the second fix, some might have covered with CVE-2020-27783 only the <noscript> and <style> part.

Thanks already,

Regards,
Salvatore

Guilherme de Almeida Suckevicz 2020-12-17 14:11:17 UTC — Comment 7

@Salvatore, as we talked by email, according to upstream the fix was split in 2 releases and were discovered together. Also, the CVE doesn't specifically say its only for certain XSS vectors, therefore, we think a new CVE is not needed in this case.

Thank you for bringing this to us!

Fedora Update System 2021-01-14 01:37:11 UTC — Comment 10

FEDORA-2020-0e055ea503 has been pushed to the Fedora 33 stable repository.
If problem still persists, please make note of it in this bug report.

Fedora Update System 2021-01-14 01:42:35 UTC Comment 11

FEDORA-2020-307946cfb6 has been pushed to the Fedora 32 stable repository.
If problem still persists, please make note of it in this bug report.

Product Security DevOps Team 2021-05-18 14:36:52 UTC Comment 12

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2020-27783

errata-xmlrpc 2021-05-18 14:50:35 UTC Comment 13

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2021:1761 https://access.redhat.com/errata/RHSA-2021:1761

errata-xmlrpc 2021-05-18 15:48:19 UTC Comment 14

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2021:1879 https://access.redhat.com/errata/RHSA-2021:1879

errata-xmlrpc 2021-05-18 15:57:02 UTC Comment 15

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2021:1898 https://access.redhat.com/errata/RHSA-2021:1898

errata-xmlrpc 2021-08-24 08:08:58 UTC Comment 16

This issue has been addressed in the following products:

Red Hat Software Collections for Red Hat Enterprise Linux 7
Red Hat Software Collections for Red Hat Enterprise Linux 7.7 EUS

Via RHSA-2021:3254 https://access.redhat.com/errata/RHSA-2021:3254

Note

You need to log in before you can comment on or make changes to this bug.