New issue

Jump to bottom

Security audit - B411 #1025

Closed nicolargo opened this issue on Feb 6, 2017 · 1 comment

Labels enhancement

Milestone Glances 3.2.1

nicolargo commented on Feb 6, 2017 • edited Owner

Description

```
bandit -r glances/
```

> Issue: [B411:blacklist] Using Fault to parse untrusted XML data is known to be vulnerable to XML attacks. Use defused.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
> Severity: High Confidence: High
> Location: glances/compat.py:91
> 90 from SimpleXMLRPCServer import SimpleXMLRPCRequestHandler, SimpleXMLRPCServer
> 91 from xmlrpclib import Fault, ProtocolError, ServerProxy, Transport
> 92 from urllib2 import urlopen, URLError

Versions

- Glances (glances -V): 2.8.1

nicolargo added the enhancement label on Feb 6, 2017

nicolargo added this to the **Glances 2.9** milestone on Feb 6, 2017

nicolargo changed the title ~~Security audit~~ Security audit - B411 on Feb 6, 2017

nicolargo modified the milestone: **Glances 2.9** on Mar 10, 2017

nicolargo commented on Mar 25, 2017 Owner Author

First idea, do not use the shell=True option. split the command line

```
In [1]: from subprocess import Popen
In [6]: cmd = 'cat README.rst | grep glances | wc -l > /tmp/titi.txt'

In [7]: Popen(cmd, shell=True)
Out[7]: <subprocess.Popen at 0x7f8b46c8c310>

In [13]: cmd_pipe = [c.split('>')[0] for c in cmd.split('|')]

In [14]: cmd_pipe
Out[14]: ['cat README.rst ', ' grep glances ', ' wc -l ']

In [15]: cmd_redir = cmd.split('>')[1]

In [16]: cmd_redir
Out[16]: ' /tmp/titi.txt'
```

and uses stdout for redirection:

```
with open('temp.txt', 'w') as output:
    server = subprocess.Popen('./server.py', stdout=output)
    server.communicate()
```

and this for pipe:

```
output=`dmesg | grep hda`
p1 = Popen(["dmesg"], stdout=PIPE)
p2 = Popen(["grep", "hda"], stdin=p1.stdout, stdout=PIPE)
p1.stdout.close()  # Allow p1 to receive a SIGPIPE if p2 exits.
output = p2.communicate()[0]
```

nicolargo modified the milestones: **Glances 2.9**, **Glances 2.9.1**, **Glances 2.9.2** on Mar 27, 2017

nicolargo modified the milestones: **Glances 2.9.2**, **Next releases**, **Glances 2.11** on May 26, 2017

nicolargo modified the milestones: **Glances 2.11**, **Glances 3.0** on Aug 27, 2017

nicolargo modified the milestones: **Glances 3.0**, **Next releases** on Sep 1, 2018

nicolargo added this to the **Glances 3.1** milestone on Sep 1, 2018

nicolargo modified the milestones: **Glances 3.1**, **Next releases**, **Glances 3.1.1** on Jan 19, 2019

nicolargo modified the milestones: **Glances 3.1.1**, **Glances 3.1.2** on Jul 24, 2019

nicolargo modified the milestones: **Glances 3.1.2**, **Next releases**, **3.1.3** on Aug 27, 2019

nicolargo modified the milestones: **Glances 3.1.3**, **Glances 3.1.4** on Oct 12, 2019

nicolargo modified the milestones: **Glances 3.1.4**, **Next releases**, **Glances 3.1.5** on Mar 10, 2020

nicolargo modified the milestones: **Glances 3.1.5**, **3.1.6** on Aug 19, 2020

nicolargo modified the milestones: **Glances 3.1.6**, **Glances 3.1.7** on Jan 23, 2021

nicolargo added a commit that referenced this issue on Apr 24, 2021

`Security audit - B411 #1025` ✕ `85d5a6b`

nicolargo closed this as completed on Apr 24, 2021

nicolargo modified the milestones: **Glances 3.1.7**, **Glances 3.2.1** on Jul 9, 2021

nicolargo added a commit that referenced this issue on Jul 9, 2021

`Security audit - B411 #1025` ✕ `9d6051b`

Assignees

No one assigned

Labels

enhancement

Projects

None yet

Milestone

Glances 3.2.1

Development

No branches or pull requests

1 participant