New issue

Jump to bottom

CVE-2017-1000501 question #90

Closed **Boran** opened this issue on Feb 20, 2018 · 3 comments

Boran commented on Feb 20, 2018

See https://security-tracker.debian.org/tracker/CVE-2017-1000501.
To fix this issue I upgraded to the latest release (7.4+dfsg-1ubuntu0.3) on my ubuntu 16.04.

Then I tried to open
http://myserver.example.com/cgi-bin/awstats.pl?config=/etc/passwd
it is still parsing /etc/passwd (even though only trying reading value pairs) and fails:

> Warning: Syntax error line 1 in file '/etc/passwd'. Config line is ignored.
> Warning: Syntax error line 2 in file '/etc/passwd'. Config line is ignored.
> Warning: Syntax error line 3 in file '/etc/passwd'. Config line is ignored.

Surely it should not open absolut paths?

The problem comes from this code, around line 1773.

```
if ( !$FileConfig ) {
        my $SiteConfigBis = File::Spec->rel2abs($SiteConfig);
        debug("Finally, try to open an absolute path : $SiteConfigBis", 2);

        if ( -f $SiteConfigBis && open(CONFIG, "$SiteConfigBis")) {
                $FileConfig = "$SiteConfigBis";
                $FileSuffix = '';
                if ($Debug){debug("Opened config: $SiteConfigBis", 2);}
                $SiteConfig=$SiteConfigBis;
        }
        else {
                if ($Debug){debug("Unable to open config file: $SiteConfigBis", 2);}
        }
}
```

In my case, the server has a name, lets say foo.example.com, it also has a DNS alias myserver.example.com. However there is no config for that domain in /etc/awstats, so it fails to find a config file it then reads a config file from the parameters - and - accepts a file that has an absolute path. Sure that should not be allowed?
Workaround: comment out the above code.

Question: what is the proper way to fix this?

avian2 commented on Feb 25, 2018 • edited Contributor

It seems that the previous fix was not complete. The same issue exists in current packages in Debian.

I've opened a bug report there: https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=891469

Another work-around until a proper fix is in place is to create an empty `/etc/awstats/awstats.conf` (so that the file gets opened and the `if ( !$FileConfig )` fails).

eldy commented on Dec 17, 2018 Owner

I think best solution is to comment all this code, around line 1773.
I made the change for awstats 7.8

eldy closed this as completed in d4d815d on Dec 17, 2018

Beuc mentioned this issue on Nov 21, 2020

Unknown security issue mentioned in 7.8 changelog #192

Closed

Beuc mentioned this issue on Dec 9, 2020

CVE-2020-35176: path traversal flaw #195

Closed

Beuc commented on Dec 9, 2020 Contributor

Hi. I opened #195 to reference an unfixed variant of this vulnerability.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants