Debian Bug report logs - #891469
awstats: Path traversal in config parameter if site config is missing (CVE-2020-29600)

awstats/7.8-2+deb11u1 (stable)
awstats/7.8-3 (testing, unstable)
awstats/7.8-2
awstats/7.8-1
awstats/7.6+dfsg-2+deb10u1 (oldstable)
awstats/7.6+dfsg-2

Package: awstats; Maintainer for awstats is Debian QA Group <packages@qa.debian.org>; Source for awstats is src:awstats (PTS, buildd, popcon).

Reported by: Tomaž Šolc <tomaz.solc@tablix.org>

Date: Sun, 25 Feb 2018 20:45:02 UTC

Severity: normal

Tags: security, upstream

Found in versions awstats/7.6+dfsg-2, awstats/7.2+dfsg-1+deb8u1, awstats/7.6+dfsg-1+deb9u1

Fixed in version awstats/7.8-1

Done: Salvatore Bonaccorso <carnil@debian.org>

Bug is archived. No further changes may be made.

Forwarded to https://github.com/eldy/awstats/issues/90

Toggle useless messages

View this report as an mbox folder, status mbox, maintainer mbox

---

Message #5 received at submit@bugs.debian.org (full text, mbox, reply):

From: Tomaž Šolc <tomaz.solc@tablix.org>
To: Debian Bug Tracking System <submit@bugs.debian.org>
Subject: awstats: Path traversal in config parameter if site config is missing.
Date: Sun, 25 Feb 2018 21:33:34 +0100

```
Package: awstats

Version: 7.6+dfsg-2

Severity: normal



Dear Maintainer,



the patch for CVE-2017-1000501 seems to have been incomplete. Please see this

report upstream:



https://github.com/eldy/awstats/issues/90



awstats will parse arbitrary files passed in the "config" parameter if the

default /etc/awstats/awstats.conf is not present. Debian package will install

awstats.conf, so a default install does not seem to be vulnerable. However it

is possible to use awstats with separate configs for different sites without

the default awstats.conf (although README.Debian recommends leaving

awstats.conf in place)



I can confirm that the reported issue exists in awstats 7.6+dfsg-2 and

7.6+dfsg-1+deb9u1.



Steps to reproduce (on Stretch)



# apt-get install awstats

# rm /etc/awstats/awstats.conf

# cp /usr/share/doc/awstats/examples/apache.conf /etc/apache2/conf-available/awstats.conf

# a2enconf awstats

# systemctl reload apache2



Visit http://localhost/cgi-bin/awstats.pl?config=/etc/passwd
```

```
-- System Information:
Debian Release: 9.3
  APT prefers stable
  APT policy: (500, 'stable')
Architecture: amd64 (x86_64)
Foreign Architectures: i386

Kernel: Linux 4.9.0-6-amd64 (SMP w/4 CPU cores)
Locale: LANG=en_US.UTF-8, LC_CTYPE=en_US.UTF-8 (charmap=UTF-8), LANGUAGE=en_US.UTF-8 (charmap=UTF-8)
Shell: /bin/sh linked to /bin/dash
Init: systemd (via /run/systemd/system)

Versions of packages awstats depends on:
ii  perl  5.24.1-3+deb9u2

Versions of packages awstats recommends:
ii  libnet-xwhois-perl  0.90-4

Versions of packages awstats suggests:
ii  apache2 [httpd]     2.4.25-3+deb9u3
pn  libgeo-ipfree-perl  <none>
ii  libnet-dns-perl     1.07-1
ii  libnet-ip-perl      1.26-1
ii  liburi-perl         1.71-1

-- Configuration Files:
/etc/awstats/awstats.conf [Errno 2] No such file or directory: '/etc/awstats/awstats.conf'

-- no debconf information
```

Message #10 received at 891469@bugs.debian.org (**full text**, **mbox**, **reply**):

From: Sylvain Beucler <beuc@beuc.net>
To: 891469@bugs.debian.org
Subject: Re: awstats: Path traversal in config parameter if site config is missing.
Date: Sun, 22 Nov 2020 00:18:46 +0100

```
Hi,

Since awstats is currently unmaintained, can you request a new CVE for
this at https://cveform.mitre.org/ ?

This way it'll be properly monitored and taken care of in distros.

Cheers!
Sylvain

On Sun, 25 Feb 2018 21:33:34 +0100 =?utf-8?b?VG9tYcW+IMWgb2xj?=
<tomaz.solc@tablix.org> wrote:
> Package: awstats
> Version: 7.6+dfsg-2
> Severity: normal
```

```
>
> Dear Maintainer,
>
> the patch for CVE-2017-1000501 seems to have been incomplete. Please see this
> report upstream:
>
> https://github.com/eldy/awstats/issues/90
>
> awstats will parse arbitrary files passed in the "config" parameter if the
> default /etc/awstats/awstats.conf is not present. Debian package will install
> awstats.conf, so a default install does not seem to be vulnerable. However it
> is possible to use awstats with separate configs for different sites without
> the default awstats.conf (although README.Debian recommends leaving
> awstats.conf in place)
>
> I can confirm that the reported issue exists in awstats 7.6+dfsg-2 and
> 7.6+dfsg-1+deb9u1.
>
> Steps to reproduce (on Stretch)
>
> # apt-get install awstats
> # rm /etc/awstats/awstats.conf
> # cp /usr/share/doc/awstats/examples/apache.conf /etc/apache2/conf-available/awstats.conf
> # a2enconf awstats
> # systemctl reload apache2
>
> Visit http://localhost/cgi-bin/awstats.pl?config=/etc/passwd
>
>
> -- System Information:
> Debian Release: 9.3
>   APT prefers stable
>   APT policy: (500, 'stable')
> Architecture: amd64 (x86_64)
> Foreign Architectures: i386
>
> Kernel: Linux 4.9.0-6-amd64 (SMP w/4 CPU cores)
> Locale: LANG=en_US.UTF-8, LC_CTYPE=en_US.UTF-8 (charmap=UTF-8), LANGUAGE=en_US.UTF-8 (charmap=UTF-8)
> Shell: /bin/sh linked to /bin/dash
> Init: systemd (via /run/systemd/system)
>
> Versions of packages awstats depends on:
> ii  perl  5.24.1-3+deb9u2
>
> Versions of packages awstats recommends:
> ii  libnet-xwhois-perl  0.90-4
>
> Versions of packages awstats suggests:
> ii  apache2 [httpd]     2.4.25-3+deb9u3
> pn  libgeo-ipfree-perl  <none>
> ii  libnet-dns-perl     1.07-1
> ii  libnet-ip-perl      1.26-1

> ii  liburi-perl         1.71-1

>

> -- Configuration Files:

> /etc/awstats/awstats.conf [Errno 2] No such file or directory: '/etc/awstats/awstats.conf'

>
```

Message #15 received at 891469@bugs.debian.org (**full text**, **mbox**, **reply**):

From: Sylvain Beucler <beuc@beuc.net>
To: 891469@bugs.debian.org
Subject: Re: awstats: Path traversal in config parameter if site config is missing.
Date: Sun, 22 Nov 2020 00:23:23 +0100

```
> Since awstats is currently unmaintained, can you request a new CVE

> for this at https://cveform.mitre.org/ ?



(I meant the awstats Debian package is currently orphaned, awstats

itself is still maintained)
```

Added tag(s) security. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Tue, 08 Dec 2020 08:27:05 GMT) (**full text**, **mbox**, **link**).

Added tag(s) upstream. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Tue, 08 Dec 2020 08:27:05 GMT) (**full text**, **mbox**, **link**).

Set Bug forwarded-to-address to 'https://github.com/eldy/awstats/issues/90'. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Tue, 08 Dec 2020 08:27:06 GMT) (**full text**, **mbox**, **link**).

Changed Bug title to 'awstats: Path traversal in config parameter if site config is missing (CVE-2020-29600)' from 'awstats: Path traversal in config parameter if site config is missing.'. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Tue, 08 Dec 2020 19:57:03 GMT) (**full text**, **mbox**, **link**).

Marked as fixed in versions awstats/7.8-1. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Sat, 12 Dec 2020 08:24:03 GMT) (**full text**, **mbox**, **link**).

Marked Bug as done Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Sat, 12 Dec 2020 08:24:03 GMT) (**full text**, **mbox**, **link**).

Message sent on to Tomaž Šolc <tomaz.solc@tablix.org>:

Bug#891469. (Sat, 12 Dec 2020 08:24:05 GMT) (**full text**, **mbox**, **link**).

Message #32 received at 891469-submitter@bugs.debian.org (**full text**, **mbox**, **reply**):

From: Salvatore Bonaccorso <carnil@debian.org>
To: control@bugs.debian.org
Cc: 891469-submitter@bugs.debian.org
Subject: closing 891469
Date: Sat, 12 Dec 2020 09:21:33 +0100

```
close 891469 7.8-1

thanks
```

Marked as found in versions awstats/7.2+dfsg-1+deb8u1. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Sat, 12 Dec 2020 08:27:02 GMT) (**full text**, **mbox**, **link**).

Marked as found in versions awstats/7.6+dfsg-1+deb9u1. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Sat, 12 Dec 2020 08:27:03 GMT) (**full text**, **mbox**, **link**).

Bug archived. Request was from Debbugs Internal Request <owner@bugs.debian.org> to internal_control@bugs.debian.org. (Tue, 12 Jan 2021 07:30:24 GMT) (**full text**, **mbox**, **link**).

Send a report that **this bug log contains spam**.
