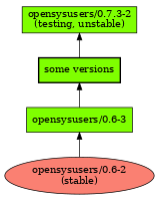
Debian Bug report logs - #992058

opensysusers: uses `eval` on data that is not supposed to be safe to eval (CVE-2021-40084)



Package: opensysusers; Maintainer for opensysusers is Andrea Pappacoda <andrea@pappacoda.it>; Source for opensysusers is src:opensysusers (PTS, buildd, popcon).

Reported by: Ansgar <ansgar@debian.org>

Date: Tue, 10 Aug 2021 09:09:02 UTC

Severity: *serious*

Tags: patch, security, upstream

Found in version opensysusers/0.6-2

Fixed in version opensysusers/0.6-3

Done: Lorenzo Puliti <plorenzo@disroot.org>

Reply or subscribe to this bug.

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: Ansgar <ansgar@debian.org>
To: Debian Bug Tracking System <submit@bugs.debian.org>
Subject: opensysusers: uses `eval` on data that is not supposed to be safe to eval
Date: Tue, 10 Aug 2021 11:07:24 +0200

```
Package: opensysusers

Version: 0.6-2

Severity: serious

Tags: security upstream

X-Debbugs-Cc: Debian Security Team <team@security.debian.org>


opensysusers uses the shell's `eval` on everything in sysusers.d like

there is no tomorrow. These files can contain shell meta-characters

that should not result in code execution, e.g., in the GECOS field.


+---

| # mkdir /etc/sysusers.d

| # echo 'u test-user - "Do not $(rm /etc/bash.bashrc)" /var/lib/test-users /bin/sh' > /etc/sysusers.d/test.conf

| # ls -l /etc/bash.bashrc

| -rw-r--r-- 1 root root 1994 Jun 22 02:26 /etc/bash.bashrc

| # systemd-sysusers # this is opensysusers

| # ls -l /etc/bash*

| ls: cannot access '/etc/bash*': No such file or directory

+---[ opensysusers 0.6-2 ]


systemd's systemd-sysuser behaves differently:


+---

| # mkdir /etc/sysusers.d

| # echo 'u test-user - "Do not $(rm /etc/bash.bashrc)" /var/lib/test-users /bin/sh' > /etc/sysusers.d/test.conf

| # ls -l /etc/bash.bashrc

| -rw-r--r-- 1 root root 1994 Jun 22 02:26 /etc/bash.bashrc

| # systemd-sysusers

| Creating group systemd-coredump with gid 999.

| Creating user systemd-coredump (systemd Core Dumper) with uid 999 and gid 999.

| Creating group test-user with gid 998.
```

```
| Creating user test-user (Do not $(rm /etc/bash.bashrc)) with uid 998 and gid 998.
| # ls -l /etc/bash.bashrc
| -rw-r--r-- 1 root root 1994 Jun 22 02:26 /etc/bash.bashrc
| # getent passwd test-user
| test-user:x:998:998:Do not $(rm /etc/bash.bashrc):/var/lib/test-users:/bin/sh
+---[ systemd 247.3-6 ]

As opensysusers is supposed to be a drop-in requirement for
systemd-sysusers it *must* behave as systemd does and not execute
data.

Ansgar
```

Changed Bug title to 'opensysusers: uses `eval` on data that is not supposed to be safe to eval (CVE-2021-40084)' from 'opensysusers: uses `eval` on data that is not supposed to be safe to eval'. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org.

(Wed, 25 Aug 2021 05:09:04 GMT) (**full text**, **mbox**, **link**).

Message #12 received at 992058@bugs.debian.org (**full text**, **mbox**, **reply**):

From: Lorenzo <plorenzo@disroot.org>
To: 992058@bugs.debian.org
Subject: Re: opensysusers: uses `eval` on data that is not supposed to be safe to eval
Date: Fri, 17 Sep 2021 19:45:51 +0200

```
Control: tags -1 patch

Hi,

On Tue, 10 Aug 2021 11:07:24 +0200 Ansgar <ansgar@debian.org> wrote:
> Package: opensysusers
> Version: 0.6-2
> Severity: serious
> Tags: security upstream
> X-Debbugs-Cc: Debian Security Team <team@security.debian.org>
>
> opensysusers uses the shell's `eval` on everything in sysusers.d like
> there is no tomorrow. These files can contain shell meta-characters
> that should not result in code execution, e.g., in the GECOS field.
>
> +---
> | # mkdir /etc/sysusers.d
> | # echo 'u test-user - "Do not $(rm /etc/bash.bashrc)"
> /var/lib/test-users /bin/sh' > /etc/sysusers.d/test.conf | # ls -l
> /etc/bash.bashrc | -rw-r--r-- 1 root root 1994 Jun 22 02:26
> /etc/bash.bashrc | # systemd-sysusers # this is opensysusers
> | # ls -l /etc/bash*
> | ls: cannot access '/etc/bash*': No such file or directory
> +---[ opensysusers 0.6-2 ]
>
> systemd's systemd-sysuser behaves differently:
>
> +---
> | # mkdir /etc/sysusers.d
```

> | # echo 'u test-user - "Do not $(rm /etc/bash.bashrc)"

> /var/lib/test-users /bin/sh' > /etc/sysusers.d/test.conf | # ls -l

> /etc/bash.bashrc | -rw-r--r-- 1 root root 1994 Jun 22 02:26

> /etc/bash.bashrc | # systemd-sysusers

> | Creating group systemd-coredump with gid 999.

> | Creating user systemd-coredump (systemd Core Dumper) with uid 999

> and gid 999. | Creating group test-user with gid 998.

> | Creating user test-user (Do not $(rm /etc/bash.bashrc)) with uid

> 998 and gid 998. | # ls -l /etc/bash.bashrc

> | -rw-r--r-- 1 root root 1994 Jun 22 02:26 /etc/bash.bashrc

> | # getent passwd test-user

> | test-user:x:998:998:Do not $(rm

> /etc/bash.bashrc):/var/lib/test-users:/bin/sh +---[systemd 247.3-6]

>

> As opensysusers is supposed to be a drop-in requirement for

> systemd-sysusers it *must* behave as systemd does and not execute

> data.

>

> Ansgar

>

Attached is a patch that sets the GECOS field without using eval: under

the assumption that the double quote character is not valid for

Type,Name,ID field it should work. Did not have the time to test it yet.

If someone has a better idea I do welcome suggestion.

Lorenzo

--- ./sysusers 2020-12-22 12:41:37.754884910 +0100

+++ ./sysusers.new   2021-09-17 19:38:32.927974348 +0200 @@ -66,10

+66,30 @@

 parse_string() {

        [-n "${l%%#*}"] || return

+   full_line=$l

-       eval "set -- $l"

+   #eval "set -- $l" # do not eval, see #992058 and CVE-2021-40084

+   set -- $l

        type="$1" name="$2" id="$3" gecos="$4" home="$5"

+   # and now set the GECOS field without eval

+   if ["${type}" = u]; then

+   if [! -z "$4"] && ["$4" != '-']; then

+   # strip everything before the first "

+   gecosplus=${full_line#*\"}

+   # now strip everything after the last "

+   gecos=${gecosplus%\"*}

+   # check if there are other valid fields after

GECOS

```
+                       gecostest=$(echo $gecosplus | grep -o '".*' -)
+                       if [ "$gecostest" = '"' ]; then
+                               home=
+                       else
+                               set -- $gecostest
+                               home=$2
+                       fi
+               fi
+       fi
+
        case "${type}" in
                [gu])
                        case "${id}" in 65535|4294967295) warninvalid;
return; esac
```

Added tag(s) patch. Request was from Lorenzo <plorenzo@disroot.org> to 992058-submit@bugs.debian.org. (Fri, 17 Sep 2021 17:48:02 GMT) (**full text**, **mbox**, **link**).

Reply sent to Lorenzo Puliti <plorenzo@disroot.org>:

You have taken responsibility. (Sun, 19 Sep 2021 16:21:05 GMT) (**full text**, **mbox**, **link**).

Message #19 received at 992058-close@bugs.debian.org (**full text**, **mbox**, **reply**):

From: Debian FTP Masters <ftpmaster@ftp-master.debian.org>
To: 992058-close@bugs.debian.org
Subject: Bug#992058: fixed in opensysusers 0.6-3
Date: Sun, 19 Sep 2021 16:18:53 +0000

```
Source: opensysusers
Source-Version: 0.6-3
Done: Lorenzo Puliti <plorenzo@disroot.org>

We believe that the bug you reported is fixed in the latest version of
opensysusers, which is due to be installed in the Debian FTP archive.

A summary of the changes between this version and the previous one is
attached.

Thank you for reporting the bug, which will now be closed.  If you
have further comments please address them to 992058@bugs.debian.org,
and the maintainer will reopen the bug report if appropriate.

Debian distribution maintenance software
pp.
Lorenzo Puliti <plorenzo@disroot.org> (supplier of updated opensysusers package)

(This message was generated automatically at their request; if you
believe that there is a problem with it please contact the archive
administrators by mailing ftpmaster@ftp-master.debian.org)

-----BEGIN PGP SIGNED MESSAGE-----
```

Hash: SHA512

Format: 1.8

Date: Sun, 19 Sep 2021 02:49:09 +0200

Source: opensysusers

Architecture: source

Version: 0.6-3

Distribution: unstable

Urgency: medium

Maintainer: Debian QA Group <packages@qa.debian.org>

Changed-By: Lorenzo Puliti <plorenzo@disroot.org>

Closes: 986015 992058

Changes:

 opensysusers (0.6-3) unstable; urgency=medium

 .

   * QA upload.

   * Update copyright years

   * Bump Standards-Version to 4.6.0, no changes

     required

   * Change section to admin

   * Update gitignore files

   * quilt patches:

     - Stop using eval (Closes: #992058, CVE-2021-40084)

     - Create group with m action (Closes: #986015)

     - Fix wrong nologin path

Checksums-Sha1:

 1c31877659537df8d23f93c4526353e8f45a762b 1931 opensysusers_0.6-3.dsc

 3594a72a28c5f21688eaa2e43c3a9eab7ef530e8 5092 opensysusers_0.6-3.debian.tar.xz

 1f7fdbca343b6284b48d1b0d8e319cdeb169b262 6449 opensysusers_0.6-3_source.buildinfo

Checksums-Sha256:

 29502aa14d77fcf34766fd3ff582ebce3d1c280d6a0f602ba36d5113e4539ca0 1931 opensysusers_0.6-3.dsc

 1167f40ebeea3d72ac93faaeb63755706c63aaffc68d187f86a172e1bfc8fd74 5092 opensysusers_0.6-3.debian.tar.xz

 86b035e65932988c79c2da63619ab921004a3bf9e5e760eda0f2880b327a0954 6449 opensysusers_0.6-3_source.buildinfo

Files:

 fcbdc59f22dbe6a970362224d8990b8d 1931 admin optional opensysusers_0.6-3.dsc

 aefdcbd74b2b6113c0b0a066be8933b2 5092 admin optional opensysusers_0.6-3.debian.tar.xz

 398f01bcafddb722d0bad318697db911 6449 admin optional opensysusers_0.6-3_source.buildinfo

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEkjZVexcMh/iCHArDweDZLphvfH4FAmFHYCsACgkQweDZLphv
fH6Z+BAAh3pURpggtPhiNDjfYz80i+NYMzKLyXQlDrUOVHDCwlDeHwRPJmFgoaaM
yQvd/c626P8ICmRBhTR04EXwNOXU26EpbOiiMahpw8d4nm5S3eFlSBE/ptQ/AU2I
l9MSsVqpPBadnWQkRxVjhbBQ78u/c4CNhnGvbF1+/NDTlZTcAOuaf0FnLJFAl36m
BTbvYwU64ganLO5VciVVm/TD8KaNCyUqJ/mbJMOZLc6U9JCbb35TZEXPktcVfKAQ
+/wbPAH0Ht0xt4t2AMcIz46ek3wMb03Xz0PWHnmfMQOOnIzHSvtGWEA9ijyBvtFm
570PsDdTXEpqVPRK4pMzg+XqHu9ZqRgbQs6ymMFCQ8ouGVAuR+fcrRRDqv5By96+
7gfih6Hb72+Ulq9CMLrYlX+DDeDETKxhIjzVMofQcaOc8eGfoSryih7RlvxjBOA5
dZguBuqGTlOP+91WtFRx63HNmZS1kMT+JKB6yJn0yYnoAOxL+0N7Bhu+8fUV/0L5
s7p6jhrEaaDWwG6eEE+QFrtc1AUO8YWUkOo6g5I3pv1ONJclyUt6N2Qz5Eu4r5nv
/J7+HdzFBWabhYLs9zgemr5wODONVI3weQVWYzPnRbG3fEugevGLKlVIvRiEvqz1

Mvps+gjelHzzQrR8qzgNzFlGOnuOnlW5OgYoaP20LGxCiq8whAg=

=MRO9

-----END PGP SIGNATURE-----
