New issue

Jump to bottom

[CVE-2020-29668] Unauthorised full access via SOAP API due to illegal cookie #1041

Closed **balert** opened this issue on Nov 24, 2020 · 5 comments · Fixed by #1044

Labels bug security

Milestone 6.2.60

balert commented on Nov 24, 2020

Version

v6.2.56-1.el7 on Centos 7.8.2003

Installation method

Centos package

Expected behavior

permission denied

Actual behavior

error message and action actually executed anyways.

Additional information

In our setup we have a problem with incorrect cookies via the SOAP API of sympa.
If the SOAP request contains a correct cookie everything works as expected -> request executed
If the SOAP request contains a correct but outdated cookie, everything works as expected -> request correctly denied.

If the SOAP request contains an arbitrary string as cookie (e.g. "asdkjasdljkahsdlkjh"), SOAP replies with an error ("Undefined session ID in cookie") but STILL executes every requests we make. By this we can add email adresses to lists without authentication, any operation we tried was still successful.

We could hotfix the problem by inserting a die(); command into /usr/share/sympa/lib/Sympa/WWW/Session.pm:129 like this:

```
    my $session_id = _cookie2id($cookie);
    unless ($session_id) {
        $log->syslog('info', 'Undefined session ID in cookie "%s"', $cookie);
        die('nothing');
        return undef;
    }
```

ikedas commented on Nov 24, 2020 Member

Hi **@balert** , could you please show what you did, such as detailed commands you executed?

ikedas added the bug label on Nov 24, 2020

balert commented on Nov 26, 2020 Author

we sent a SOAP request like this:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:sympasoap" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
   <soapenv:Header/>
   <soapenv:Body>
      <urn:authenticateAndRun soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
         <email xsi:type="xsd:string">mail@example.org</email>
         <cookie xsi:type="xsd:string">randomstring</cookie>
         <service xsi:type="xsd:string">review</service>
         <parameters xsi:type="wsdl:ArrayOfString" soapenc:arrayType="xsd:string[]" xmlns:wsdl="https://lists.example.org/sympa/wsdl">
                        <item>list@example.org</item>>
         </parameters>
      </urn:authenticateAndRun>
   </soapenv:Body>
</soapenv:Envelope>
```

racke added the security label on Nov 26, 2020

racke commented on Nov 26, 2020 Contributor

If that is true it would be a big hole. I'm going to try to reproduce it.

racke commented on Nov 27, 2020 • edited

Contributor

I can confirm the problem. You need to know the listname and the email that is allowed to see the subscribers (e.g. the owner of the list.

Reproduce that with the client test script:

```
/usr/local/sympa/bin/sympa_soap_client.pl
   --soap_url=https://lists.example.com/sympasoap
   --service=review
   --service_parameters=demo-list
   --user_email=demo@cart.pm
   --session_id=nevairbe
```

racke added a commit to racke/sympa that referenced this issue on Nov 27, 2020

`Properly check email and session id in authenticateAndRun SOAP call (s… …` ✓ 52157b5

racke mentioned this issue on Nov 27, 2020

Properly check email and session id in authenticateAndRun SOAP call (#1041) #1044

Merged

ikedas added the **on going** label on Nov 30, 2020

ikedas added this to the **6.2.60** milestone on Nov 30, 2020

ikedas closed this as completed in #1044 on Dec 7, 2020

ikedas added a commit that referenced this issue on Dec 7, 2020

`Merge pull request #1044 from racke/pr/soap-api-access-fix by racke …` ✓ 4dacc82

carnil commented on Dec 10, 2020

This issue has been assigned CVE-2020-29668.

👍 1

ikedas changed the title ~~Unauthorised full access via SOAP API due to illegal cookie~~ **[CVE-2020-29668Unauthorised full access via SOAP API due to illegal cookie** on Dec 11, 2020

ikedas changed the title ~~[CVE-2020-29668Unauthorised full access via SOAP API due to illegal cookie~~ **[CVE-2020-29668] Unauthorised full access via SOAP API due to illegal cookie** on Dec 11, 2020

ikedas pinned this issue on Dec 11, 2020

uqs pushed a commit to freebsd/freebsd-ports that referenced this issue on Jan 6, 2021

`mail/sympa: update 6.2.58 -> 6.2.60, security update CVE-2020-29668 …` 3ade5e0

uqs pushed a commit to freebsd/freebsd-ports that referenced this issue on Jan 6, 2021

`MFH: r560539 …` 433cc3e

uqs pushed a commit to freebsd/freebsd-ports that referenced this issue on Jan 6, 2021

`mail/sympa: update 6.2.58 -> 6.2.60, security update CVE-2020-29668 …` 06ea1ee

Jehops pushed a commit to Jehops/freebsd-ports-legacy that referenced this issue on Jan 6, 2021

`mail/sympa: update 6.2.58 -> 6.2.60, security update CVE-2020-29668 …` 0b28ebf

uqs pushed a commit to freebsd/freebsd-ports that referenced this issue on Apr 1, 2021

`MFH: r560539 …` b4c2913

ikedas unpinned this issue on Apr 18, 2021

ikedas removed the **on going** label on Jul 6, 2021

Assignees

No one assigned

Labels

bug security

Projects

None yet

Milestone

6.2.60

Development

Successfully merging a pull request may close this issue.

Properly check email and session id in authenticateAndRun SOAP call (#1041)
racke/sympa

4 participants