~~Bug 1199512 - (CVE-2022-21952) VUL-0: CVE-2022-21952: SUMA unauthenticated remote DoS via resource exhaustion~~

Status:	RESOLVED FIXED
Classification:	Novell Products
Product:	SUSE Security Incidents
Component:	Audits
Version:	unspecified
Hardware:	Other Other
Priority:	P3 - Medium **Severity**: Normal
Target Milestone:	---
Assigned To:	Can Bayburt
QA Contact:	Security Team bot
URL:	https://smash.suse.de/issue/331772/
Whiteboard:	CVSSv3.1:SUSE:CVE-2022-21952:7.5:(AV:...
Keywords:	
Depends on:	
Blocks:	1197339
	Show dependency tree / graph

- Create test case
- Clone This Bug

Reported:	2022-05-13 09:08 UTC by Paolo Perego
Modified:	2022-07-25 08:06 UTC (History)
CC List:	13 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.

Paolo Perego 2022-05-13 09:08:38 UTC Description

```
On SUMA, the endpoint /rhn/manager/frontend-log takes a text as a POST parameter
and then it writes on /var/log/rhn/rhn_web_frontend.log file.
This file is then used by supportconfig to create archive in case of debugging
purposes.

The input is in the form of {'level':'error', 'message':'Message'}. The attacker
can control the severity level of the log message and the text.
The file implementing the log facility is https://github.com/uyuni-
project/uyuni/blob/master/java/code/src/com/suse/manager/webui/controllers/FrontendLo
```

The problem is that this endpoint is not restricted, there is no throttling mechanism end it doesn't sanitize incoming input so it is possible for an unauthenticated user to write arbitrary contents in the log file.

e.g:
2022-05-13 10:24:04,855 [ajp-nio-0:0:0:0:0:0:0:1-8009-exec-8] ERROR com.suse.manager.webui.controllers.FrontendLogController - [no-logged-user - python-requests/2.27.1] - <?php phpinfo(); ?>
2022-05-13 10:24:43,911 [ajp-nio-0:0:0:0:0:0:0:1-8009-exec-4] ERROR com.suse.manager.webui.controllers.FrontendLogController - [no-logged-user - python-requests/2.27.1] - <script>alert();</script>
2022-05-13 10:24:51,944 [ajp-nio-0:0:0:0:0:0:0:1-8009-exec-9] ERROR com.suse.manager.webui.controllers.FrontendLogController - [no-logged-user - python-requests/2.27.1] - <script>alert(document.cookies);</script>
2022-05-13 10:25:03,741 [ajp-nio-0:0:0:0:0:0:0:1-8009-exec-2] ERROR com.suse.manager.webui.controllers.FrontendLogController - [no-logged-user - python-requests/2.27.1] - <script>alert('d');</script>

Since there is no direct utilization of that file content in the web ui, a log poisoning attack is not possible. However, since there is no a logrotate policy for that file, is it possible to exhaust available disk space by injecting big portions of text.

Paolo Perego 2022-05-13 09:09:08 UTC Comment 1

Created attachment 858890 [details]
The exploit poc

Paolo Perego 2022-05-13 09:12:12 UTC Comment 2

The log file is consumed here: https://github.com/uyuni-project/uyuni/blob/master/python/spacewalk/satellite_tools/spacewalk-debug#L198

cp -fapd /var/log/rhn/*.log* $DIR/rhn-logs/rhn

So to achieve a log poisoning attack seems not to be possible (unless the log is transfered to a third party system and consumed there)

Johannes Segitz 2022-05-16 11:03:36 UTC Comment 7

Please use CVE-2022-21952 for this

Paolo Perego 2022-05-27 10:00:38 UTC Comment 20

CVSS score for this is 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Paolo Perego 2022-06-20 14:21:52 UTC Comment 32

Patch is released, we can lift the embargo

Swamp Workflow Management 2022-06-21 10:18:17 UTC Comment 33

SUSE-SU-2022:2145-1: An update that solves 5 vulnerabilities, contains two features and has 33 fixes is now available.

Category: security (important)
Bug References:
1173527,1182742,1189501,1190535,1191143,1192850,1193032,1193238,1193707,1194262,11944

CVE References: CVE-2022-21698,CVE-2022-21724,CVE-2022-21952,CVE-2022-26520,CVE-2022-31248
JIRA References: SLE-24238,SLE-24239
Sources used:
SUSE Linux Enterprise Module for SUSE Manager Server 4.1 (src): golang-github-QubitProducts-exporter_exporter-0.4.0-150200.6.12.2, golang-github-lusitaniae-apache_exporter-0.7.0-150200.2.6.2, golang-github-prometheus-node_exporter-1.3.0-150200.3.9.3, patterns-suse-manager-4.1-150200.6.12.2, postgresql-jdbc-42.2.10-150200.3.8.2, prometheus-exporters-formula-0.9.5-150200.3.31.2, prometheus-formula-0.3.7-150200.3.21.2, py27-compat-salt-3000.3-150200.6.24.2, spacecmd-4.1.18-150200.4.39.3, spacewalk-backend-4.1.31-150200.4.50.4, spacewalk-java-4.1.46-150200.3.71.5, spacewalk-setup-4.1.11-150200.3.18.2, spacewalk-utils-4.1.20-150200.3.30.2, spacewalk-web-4.1.34-150200.3.47.6, subscription-matcher-0.28-150200.3.15.2, susemanager-4.1.36-150200.3.52.1, susemanager-doc-indexes-4.1-150200.11.55.4, susemanager-docs_en-4.1-150200.11.55.2, susemanager-schema-4.1.26-150200.3.45.4, susemanager-sls-4.1.36-150200.3.64.2

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 2022-06-21 10:21:19 UTC Comment 34

SUSE-SU-2022:2143-1: An update that solves four vulnerabilities and has 28 fixes is now available.

Category: security (moderate)
Bug References:
1182742,1189501,1190535,1192850,1193032,1193238,1193707,1194262,1194447,1194594,1194

CVE References: CVE-2022-21724,CVE-2022-21952,CVE-2022-26520,CVE-2022-31248
JIRA References:
Sources used:
SUSE Manager Server 4.1 (src): release-notes-susemanager-4.1.15-150200.3.80.1
SUSE Manager Retail Branch Server 4.1 (src): release-notes-susemanager-proxy-4.1.15-150200.3.56.1
SUSE Manager Proxy 4.1 (src): release-notes-susemanager-proxy-4.1.15-150200.3.56.1

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 2022-06-21 10:23:24 UTC Comment 35

SUSE-SU-2022:2144-1: An update that solves three vulnerabilities and has 18 fixes is now available.

Category: security (important)
Bug References:
1187333,1191143,1192550,1193707,1194594,1195710,1196702,1197400,1197438,1197449,1197

CVE References: CVE-2021-44906,CVE-2022-21952,CVE-2022-31248
JIRA References:
Sources used:
SUSE Linux Enterprise Module for SUSE Manager Server 4.2 (src): inter-server-sync-0.2.2-150300.8.17.1, prometheus-formula-0.6.2-150300.3.14.1, salt-netapi-client-0.19.0-150300.3.6.1, smdba-1.7.10-0.150300.3.6.1, spacecmd-4.2.17-150300.4.21.4, spacewalk-backend-4.2.22-150300.4.23.1, spacewalk-certs-tools-4.2.16-150300.3.18.3, spacewalk-java-4.2.38-150300.3.35.1, spacewalk-utils-4.2.16-150300.3.15.5, spacewalk-web-4.2.27-150300.3.21.7, supportutils-plugin-salt-1.2.0-150300.3.3.1, susemanager-4.2.32-150300.3.31.1, susemanager-doc-indexes-4.2-150300.12.27.6, susemanager-docs_en-4.2-150300.12.27.1, susemanager-schema-4.2.22-150300.3.21.6, susemanager-sls-4.2.23-150300.3.25.4, susemanager-sync-data-4.2.12-150300.3.18.3, virtual-host-gatherer-1.0.23-150300.3.3.1

```
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 2022-06-21 10:28:09 UTC Comment 36

```
SUSE-SU-2022:2144-1: An update that solves three vulnerabilities and has 18 fixes
is now available.

Category: security (important)
Bug References:
1187333,1191143,1192550,1193707,1194594,1195710,1196702,1197400,1197438,1197449,11974

CVE References: CVE-2021-44906,CVE-2022-21952,CVE-2022-31248
JIRA References:
Sources used:
SUSE Linux Enterprise Module for SUSE Manager Server 4.2 (src):    inter-server-
sync-0.2.2-150300.8.17.1, prometheus-formula-0.6.2-150300.3.14.1, salt-netapi-
client-0.19.0-150300.3.6.1, smdba-1.7.10-0.150300.3.6.1, spacecmd-4.2.17-
150300.4.21.4, spacewalk-backend-4.2.22-150300.4.23.1, spacewalk-certs-tools-
4.2.16-150300.3.18.3, spacewalk-java-4.2.38-150300.3.35.1, spacewalk-utils-4.2.16-
150300.3.15.5, spacewalk-web-4.2.27-150300.3.21.7, supportutils-plugin-salt-1.2.0-
150300.3.3.1, susemanager-4.2.32-150300.3.31.1, susemanager-doc-indexes-4.2-
150300.12.27.6, susemanager-docs_en-4.2-150300.12.27.1, susemanager-schema-4.2.22-
150300.3.21.6, susemanager-sls-4.2.23-150300.3.25.4, susemanager-sync-data-4.2.12-
150300.3.18.3, virtual-host-gatherer-1.0.23-150300.3.3.1
SUSE Linux Enterprise Module for SUSE Manager Proxy 4.2 (src):    spacecmd-4.2.17-
150300.4.21.4, spacewalk-backend-4.2.22-150300.4.23.1, spacewalk-certs-tools-
4.2.16-150300.3.18.3, spacewalk-web-4.2.27-150300.3.21.7, supportutils-plugin-salt-
1.2.0-150300.3.3.1

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.
```