~~Bug 1199629 - (CVE-2022-31248) VUL-0: CVE-2022-31248: SUMA user enumeration via weak error message~~

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: Welder Luz
QA Contact: Security Team bot

URL: https://github.com/SUSE/spacewalk/iss...
Whiteboard: CVSSv3.1:SUSE:CVE-2022-31248:5.3:(AV:...
Keywords:

Depends on:
Blocks: 1197339
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2022-05-17 13:48 UTC by Paolo Perego
Modified: 2022-09-08 13:52 UTC (History)
CC List: 11 users (show)

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

Flags: marina.latini: SHIP_STOPPER?

Attachments

the exploit code for testing (1.60 KB, text/x-python) Details
2022-05-17 14:34 UTC, Paolo Perego

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

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

Paolo Perego 2022-05-17 13:48:30 UTC Description

```
The /rhn/help/ForgotCredentials.do offer two different facilities to retrieve login
information.

The first is asking for a password reset, using your login handle and the email
address.

The second is submitting your email address if the user can't remember the login
handle.
Unfortunately, the web application is too detailed in the error message. It is
```

possible to enumerate registered emails simply by submitting to the page.

It has been found that this service is available also using a plain GET HTTP request and that it answers 302, redirecting to the homepage in case of a valid email address and it returns 200, with an error message in case of not a present email address.
This turn the exploit code much easier to write.

Paolo Perego 2022-05-17 14:34:45 UTC Comment 3

Created attachment 858989 [details]
the exploit code for testing

Paolo Perego 2022-05-24 07:39:47 UTC Comment 8

I was pretty convinced I did already, sorry for that.

We set CRD to 2022-06-20

Paolo Perego 2022-05-27 10:01:37 UTC Comment 10

CVSS is 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Johannes Segitz 2022-05-27 12:36:44 UTC Comment 12

Please use CVE-2022-31248 for this

Paolo Perego 2022-06-20 14:21:29 UTC Comment 24

Patch is released - We can lift the embargo.

Swamp Workflow Management 2022-06-21 10:18:31 UTC Comment 25

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 10:21:29 UTC Comment 26

```
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 10:23:28 UTC Comment 27

```
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

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 10:28:13 UTC Comment 28

```
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.
```

Swamp Workflow Management 2022-07-27 19:18:02 UTC Comment 32

```
SUSE-SU-2022:2567-1: An update that solves one vulnerability and has 43 fixes is
now available.

Category: security (important)
Bug References:
1179962,1182742,1189501,1192850,1193032,1193238,1194262,1194394,1196977,1197429,11975

CVE References: CVE-2022-31248
JIRA References:
Sources used:
SUSE Manager Server 4.2 (src):    release-notes-susemanager-4.2.8-150300.3.51.2
SUSE Manager Retail Branch Server 4.2 (src):    release-notes-susemanager-proxy-
4.2.8-150300.3.40.2
SUSE Manager Proxy 4.2 (src):    release-notes-susemanager-proxy-4.2.8-
150300.3.40.2

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 2022-07-27 19:22:44 UTC Comment 33

```
SUSE-SU-2022:2568-1: An update that solves one vulnerability and has 42 fixes is
now available.

Category: security (important)
Bug References:
1179962,1182742,1189501,1192850,1193032,1193238,1194262,1194394,1196977,1197429,11975

CVE References: CVE-2022-31248
JIRA References:
Sources used:
SUSE Linux Enterprise Module for SUSE Manager Server 4.2 (src):    apache-commons-
csv-1.2-150300.3.3.2, apache-commons-math3-3.2-150300.3.3.2, drools-7.17.0-
150300.4.3.2, jakarta-commons-validator-1.1.4-21.150300.21.3.3, jose4j-0.5.1-
150300.3.3.2, kie-api-7.17.0-150300.4.3.2, mvel2-2.2.6.Final-150300.3.3.2,
optaplanner-7.17.0-150300.4.3.2, py27-compat-salt-3000.3-150300.7.7.20.2, python-
susemanager-retail-1.0.1653987003.92d4870-150300.3.3.2, smdba-1.7.10-
0.150300.3.9.2, spacecmd-4.2.18-150300.4.24.3, spacewalk-admin-4.2.11-
150300.3.12.3, spacewalk-backend-4.2.23-150300.4.26.3, spacewalk-branding-4.2.14-
150300.3.12.3, spacewalk-certs-tools-4.2.17-150300.3.21.2, spacewalk-client-tools-
4.2.19-150300.4.21.3, spacewalk-java-4.2.40-150300.3.40.2, spacewalk-search-4.2.7-
150300.3.9.2, spacewalk-setup-4.2.11-150300.3.15.2, spacewalk-utils-4.2.17-
150300.3.18.3, spacewalk-web-4.2.28-150300.3.24.3, subscription-matcher-0.29-
```

```
150300.6.9.2, susemanager-4.2.35-150300.3.36.1, susemanager-doc-indexes-4.2-
150300.12.30.3, susemanager-docs_en-4.2-150300.12.30.2, susemanager-schema-4.2.23-
150300.3.24.3, susemanager-sls-4.2.26-150300.3.30.1, susemanager-sync-data-4.2.13-
150300.3.21.2, virtual-host-gatherer-1.0.23-150300.3.6.2, woodstox-4.4.2-
150300.3.3.2, xmlpull-api-1.1.3.1-150300.3.3.2

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 2022-09-08 13:32:49 UTC Comment 35

```
SUSE-SU-2022:3194-1: An update that solves one vulnerability and has 41 fixes is
now available.

Category: security (moderate)
Bug References:
1172179,1179962,1186011,1187028,1191925,1194394,1195455,1198356,1198358,1198944,11991

CVE References: CVE-2022-31248
JIRA References:
Sources used:
SUSE Linux Enterprise Module for SUSE Manager Server 4.3 (src):    apache-commons-
csv-1.2-150400.3.3.1, apache-commons-math3-3.2-150400.3.3.1, drools-7.17.0-
150400.3.3.1, image-sync-formula-0.1.1658330139.861779d-150400.3.3.1, inter-server-
sync-0.2.3-150400.3.3.1, jakarta-commons-validator-1.1.4-21.150400.21.3.4, jose4j-
0.5.1-150400.3.3.1, kie-api-7.17.0-150400.3.3.1, mvel2-2.2.6.Final-150400.3.3.1,
optaplanner-7.17.0-150400.3.3.1, python-susemanager-retail-1.0.1658330139.861779d-
150400.3.3.1, python-urlgrabber-4.1.0-150400.3.3.1, reprepro-5.3.0-150400.3.3.1,
salt-netapi-client-0.20.0-150400.3.3.5, smdba-1.7.10-0.150400.4.3.1, spacecmd-
4.3.14-150400.3.3.2, spacewalk-4.3.5-150400.3.3.2, spacewalk-backend-4.3.15-
150400.3.3.5, spacewalk-certs-tools-4.3.14-150400.3.3.2, spacewalk-client-tools-
4.3.11-150400.3.3.4, spacewalk-config-4.3.9-150400.3.3.3, spacewalk-java-4.3.35-
150400.3.3.5, spacewalk-search-4.3.6-150400.3.3.3, spacewalk-setup-4.3.10-
150400.3.3.3, spacewalk-utils-4.3.13-150400.3.3.3, spacewalk-web-4.3.23-
150400.3.3.4, subscription-matcher-0.29-150400.3.3.1, susemanager-4.3.18-
150400.3.3.2, susemanager-build-keys-15.4.3-150400.3.3.1, susemanager-docs_en-4.3-
150400.9.3.1, susemanager-schema-4.3.13-150400.3.3.3, susemanager-sls-4.3.24-
150400.3.3.1, uyuni-common-libs-4.3.5-150400.3.3.2, virtual-host-gatherer-1.0.23-
150400.3.3.1, woodstox-4.4.2-150400.3.3.1, xmlpull-api-1.1.3.1-150400.3.3.1

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 2022-09-08 13:52:28 UTC Comment 36

```
SUSE-RU-2022:3182-1: An update that has 42 recommended fixes can now be installed.

Category: recommended (moderate)
Bug References:
1172179,1179962,1186011,1187028,1191925,1194394,1195455,1198356,1198358,1198944,11991

CVE References:
JIRA References:
Sources used:
SUSE Manager Server 4.3 (src):    release-notes-susemanager-4.3.1-150400.3.8.1
SUSE Manager Retail Branch Server 4.3 (src):    release-notes-susemanager-proxy-
4.3.1-150400.3.6.1
SUSE Manager Proxy 4.3 (src):    release-notes-susemanager-proxy-4.3.1-150400.3.6.1

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.
```

First Last Prev Next This bug is not in your last search results.

Format For Printing - XML - Clone This Bug - Top of page