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

~~Bug 1204716 - (CVE-2022-43753) VUL-0: CVE-2022-43753: SUMA/UYUNI arbitrary file disclosure vulnerability in ScapResultDownload~~

Status:	RESOLVED FIXED
Classification:	Novell Products
Product:	SUSE Security Incidents
Component:	Incidents
Version:	unspecified
Hardware:	Other Other
Priority:	P5 - None **Severity**: Normal
Target Milestone:	---
Assigned To:	Kevin Walter
QA Contact:	Security Team bot
URL:	
Whiteboard:	CVSSv3.1:SUSE:CVE-2022-43753:5.0:(AV:...
Keywords:	
Depends on:	
Blocks:	1201713
	Show dependency tree / graph

- Create test case
- Clone This Bug

Reported:	2022-10-25 16:39 UTC by Paolo Perego
Modified:	2022-11-04 17:39 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.

Paolo Perego 2022-10-25 16:39:25 UTC Description

During a SUMA/UYUNI audit, an arbitrary file disclosure vulnerability it has been found in the ScapResultDownload servlet.

When downloading the openscap result for a given system, it is possible to evade from the location where the report is created and access arbitrary files.

On a default installation, tomcat is running as a non-privileged user process, so the impact on the file system confidentiality is for files viewable by tomcat user, for groups www, susemanager and tomcat and for files viewable by anyone.

To exploit this vulnerability there is no need for a particular script but an

```
authenticated SUMA session is needed.

CVSS is 5.0:
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:


PoC
https://server_ip/rhn/systems/details/audit/ScapResultDownload.do?
sid=1000010000&xid=1&name=../../../../../../../etc/passwd

Mitigation
The getAbsolutePath() method in the ScapResultFile class should discard characters
to evade from report output directory
```

Johannes Segitz 2022-10-26 06:56:50 UTC Comment 2

```
Please use CVE-2022-43753 for this
```

Paolo Perego 2022-10-26 09:26:35 UTC Comment 7

```
CRD: 2022-11-04 15.00 UTC
```

Paolo Perego 2022-11-04 16:13:41 UTC Comment 10

```
Fixed versions: SUMA 4.3.2, 4.2.10 and Uyuni-2022.10
```

Swamp Workflow Management 2022-11-04 17:30:14 UTC Comment 11

```
SUSE-SU-2022:3880-1: An update that fixes three vulnerabilities is now available.

Category: security (critical)
Bug References: 1204543,1204716,1204741
CVE References: CVE-2022-31255,CVE-2022-43753,CVE-2022-43754
JIRA References:
Sources used:
SUSE Linux Enterprise Module for SUSE Manager Server 4.3 (src):    spacewalk-java-
4.3.39-150400.3.11.1

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 2022-11-04 17:32:33 UTC Comment 12

```
SUSE-SU-2022:3878-1: An update that solves three vulnerabilities and has 18 fixes
is now available.

Category: security (critical)
Bug References:
1195624,1197724,1199726,1200596,1201059,1201788,1202167,1202729,1202785,1203283,12034

CVE References: CVE-2022-31255,CVE-2022-43753,CVE-2022-43754
JIRA References:
Sources used:
SUSE Linux Enterprise Module for SUSE Manager Server 4.2 (src):    hub-xmlrpc-api-
0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-
150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-
3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-
4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-
4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-
150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-
```

```
150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-
150300.3.30.3, susemanager-sls-4.2.28-150300.3.36.2

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 2022-11-04 17:39:25 UTC Comment 13

```
SUSE-SU-2022:3879-1: An update that solves three vulnerabilities and has 18 fixes
is now available.

Category: security (critical)
Bug References:
1195624,1197724,1199726,1200596,1201059,1201788,1202167,1202729,1202785,1203283,12034

CVE References: CVE-2022-31255,CVE-2022-43753,CVE-2022-43754
JIRA References:
Sources used:
SUSE Manager Server 4.2 (src):    release-notes-susemanager-4.2.10-150300.3.57.1
SUSE Manager Retail Branch Server 4.2 (src):    release-notes-susemanager-proxy-
4.2.10-150300.3.46.1
SUSE Manager Proxy 4.2 (src):    release-notes-susemanager-proxy-4.2.10-
150300.3.46.1

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