Security Advisory 2022-007

Serious Vulnerability in All Major Linux Distributions

January 27, 2022 — v1.0

TLP:WHITE

History:

- 27/01/2022 — v1.0 – Initial publication

Summary

On January 25, Polkit’s authors released a patch for their software fixing a severe vulnerability that could lead to local privilege escalation on all Major Linux distributions (including Ubuntu, Debian, Fedora, and CentOS) [1,2].

Exploits for this vulnerability already exist in the wild.

It is recommended to update Linux distributions as soon as possible.

Technical Details

The vulnerability, identified as CVE-2021-4034, has a severity score of 7.8 out of 10. This is a memory corruption vulnerability caused by the way arguments are read by the pkexec component of Polkit. This would allow to reintroduce an unsecure (because it leads to the execution of arbitrary libraries) environment variable into pkexec’s environment that would normally be removed before the program execution [2].

This vulnerability is really easy to exploit.

Affected Products

All versions of Polkit since the first introduction of pkexec are vulnerable (since version 0.113 from 2009). The authors have integrated a fix in the last published release, but has not created a specific release number [3].
Recommendations

CERT-EU recommends updating all running Linux distributions that provided a backport of the fix [4, 5, 6, 7]:

- Ubuntu 14.04, 16.04 ESM
- Ubuntu 18.04, 20.04, and 21.04
- RedHat at Workstation and Enterprise products for supported architectures, as well as for extended life cycle support, TUS, and AUS.
- Debian Stretch, Buster, Bellseye, unstable

A reboot might be necessary.

Workaround

A temporary mitigation is available to prevent from the privilege escalation vulnerability:

```bash
chmod 0755 /usr/bin/pkexec
```

Analysis

CERT-EU also recommends searching for exploitation attempts by checking the logs against the following strings:

```
"The value for the SHELL variable was not found the /etc/shells file"
and/or
"The value for environment variable [...] contains suspicious content."
```

However, Qualys notes that exploiting PwnKit is possible without leaving a trace [2].

References