~~Bug 1201949 - VUL-0: CVE-2022-37030: gromox: potential local privilege escalation~~

Status: RESOLVED FIXED

- Create test case
- Clone This Bug

Classification:	openSUSE
Product:	openSUSE Tumbleweed
Component:	Security
Version:	Current
Hardware:	x86-64 Linux
Priority:	P3 - Medium **Severity**: Normal (vote)
Target Milestone:	---
Assigned To:	Security Team bot
QA Contact:	E-mail List
URL:	
Whiteboard:	
Keywords:	
Depends on:	
Blocks:	~~1200165~~ Show dependency tree / graph

Reported:	2022-07-28 09:30 UTC by Filippo Bonazzi
Modified:	2022-08-05 07:58 UTC (History)
CC List:	0 users
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.

Filippo Bonazzi 2022-07-28 09:30:01 UTC   Description

```
During an audit of Gromox for inclusion in openSUSE Tumbleweed, a potential local
privilege escalation was found as described in bsc#1200165.
```

Filippo Bonazzi 2022-07-28 10:26:42 UTC   Comment 1

```
The following report describes a local privilege escalation vulnerability in
Gromox[0] version 1.27 (latest). The vulnerability probably applies to previous
versions as well, since it has to do with the way the application is packaged.

# Introduction
```

Gromox is the central groupware server component of grommunio[1]. It is capable of serving as a replacement for Microsoft Exchange and compatibles.

Among its many features, Gromox provides a PAM module to authenticate non-Gromox processes to an authentication backend such as MySQL or LDAP. The PAM module allows runtime loading of plugins, and its configuration lives in `/etc/gromox/pam` or `/etc/gromox`.

The interaction between this PAM module, its runtime loading of plugins and their configuration causes the vulnerability described in this report.

# The Vulnerability

The RPM spec file packages the `/etc/gromox` directory with ownership `root:gromox` and mode 775, i.e. the directory is writeable by the unprivileged `gromox` group.

The directory contains, among others, the configuration file for the PAM module. When the authentication hook of the PAM module is invoked, the module loads the `/etc/gromox/pam.cfg` configuration file, which can contain a path and a list of filenames to be used to load plugins. The plugins are regular .so shared objects, which are then executed by the PAM module.

It is therefore possible for the `gromox` group to effectively have the PAM stack run arbitrary code upon execution of the `pam_gromox.so` module.

Assuming that the PAM stack is run as root, as it is likely, this results in the unprivileged `gromox` group being able to execute arbitrary code as root.

# Proof of Concept Exploit

Attached is a proof of concept setup that has been tested on current openSUSE distributions.
The only precondition for the exploit is that gromox is installed and a target user is in the `gromox` group.

# Suggested Fix

In order to prevent privilege escalation, an unprivileged user cannot be allowed to control paths and filenames that will be executed by other users (`root` in the worst case).

Probably the best thing to do is to set the `/etc/gromox` folder ownership to `root:root` and mode 755 rather than 775, and only allow privileged users to modify the configuration.

# References

[0] https://gromox.com/
[1] https://grommunio.com/

Filippo Bonazzi 2022-08-01 17:12:26 UTC Comment 2

The issue has been assigned CVE-2022-37030.

Filippo Bonazzi 2022-08-05 07:58:26 UTC Comment 3

CVE has been made public and report has been posted to OSS[0].

Closing this as we are unaffected.

[0] https://www.openwall.com/lists/oss-security/2022/08/04/1

First Last Prev Next This bug is not in your last search results. Format For Printing - XML - Clone This Bug - Top of page