Bug 1964129 (CVE-2021-35939) - CVE-2021-35939 rpm: checks for unsafe symlinks are not performed for intermediary directories

Keywords: Security ×

Status: NEW

Alias: CVE-2021-35939

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 1969333 1969334 1969335 1978170 1969804 1969805 1969806 ~~1977848~~ 1978167 1978169 1978171 2003067 2070455

Blocks: 1964123 1977374

TreeView+ depends on / blocked

Reported: 2021-05-24 19:00 UTC by msiddiqu

Modified: 2022-12-01 10:46 UTC (History)

CC List: 11 users (show)

Fixed In Version: rpm 4.18.0

Doc Type: If docs needed, set a value

Doc Text: It was found that the fix for CVE-2017-7500 and CVE-2017-7501 was incomplete: the check was only implemented for the parent directory of the file to be created. A local unprivileged user who owns another ancestor directory could potentially use this flaw to gain root privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

Clone Of:

Environment:

Last Closed:

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

msiddiqu 2021-05-24 19:00:44 UTC — Description

In response to CVE-2017-7500 and CVE-2017-7501, it was decided that the policy of RPM is "Only follow directory symlinks owned by target directory owner or root." [1]. This check was only implemented for the parent directory of the file to be created. If an untrusted user owns another ancestor directory, the problem remains unfixed.

An actual exploit requires that a similar directory structure exists both at the location where RPM operates and for the files the attacker wants to get control over. Packages with such paths do exist in the real world, however. For example, in openSUSE both matomo and icinga2 ship a 'Pdo/Mysql.php' somewhere in the file system, with different ownership. A compromised 'matomo' user can create a symlink /srv/www/matomo/core/Tracker/Db -> /usr/share/icingaweb2/library/vendor/Zend/Db/Adapter/ and on the next update of matomo, RPM would replace the 'Pdo/Mysql.php' of icinga2 and give ownership of it to the 'matomo' user.

A fix for this requires a messy ball of code using O_PATH to manually walk the whole directory structure and manually resolving symlinks, like in [1] and [2].

References:

1: https://github.com/systemd/systemd/blob/a5648b809457d120500b2acb18b31e2168a4817a/src/basic/fs-util.c#L716
2: https://build.suse.de/package/view_file/SUSE:Maintenance:13179/permissions.SUSE_SLE-15-SP1_Update/0007-chkstat-fix-privesc-CVE-2019-3690.patch?expand=1
3. https://bugzilla.suse.com/show_bug.cgi?id=1157883

Mauro Matteo Cascella 2021-06-30 15:22:06 UTC — Comment 4

Created rpm tracking bugs for this issue:

Affects: fedora-all [~~Bug 1977848~~]

Mauro Matteo Cascella 2021-07-07 16:24:29 UTC — Comment 9

This flaw, along with CVE-2021-35937 and CVE-2021-35938, belong to a set of complex issues that may allow an unprivileged user to trick RPM into modifying root-owned files during installation, due to race conditions and/or symlink attacks. These issues do not have a solution upstream. Fixing would require rather involved refactoring of RPM internals.

Note that in this context, unprivileged users are actually system accounts (like the pcpqa user mentioned in one of the SUSE bugs) that are usually more tightly controlled than ordinary users. In general, access to files and directories installed by RPMs requires high privileges. Regular users should not be allowed to manipulate RPM artifacts during installation. A local attacker would first need to compromise a system account in order to exploit these flaws, thus reducing the overall impact considerably.

Panu Matilainen 2022-05-13 07:35:37 UTC — Comment 13

This is considered fixed in RPM 4.18 (https://rpm.org/wiki/Releases/4.18.0) which is currently in alpha stage of the release process, final version is expected in Q3.

Mauro Matteo Cascella 2022-11-28 11:42:50 UTC — Comment 14

Upstream PR & commit:
https://github.com/rpm-software-management/rpm/pull/1919
https://github.com/rpm-software-management/rpm/commit/96ec957e281220f8e137a2d5eb23b83a6377d556

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