



not when it downloading over HTTP) can send a Content-Disposition header to make pacman place the file anywhere in the filesystem, potentially leading to arbitrary root code execution. Notably, this bypasses pacman's package signature checking. This occurs in curl_download_internal in lib/libalpm/dload.c."> " due to an unsanitized file name received from a Content-Disposition header. pac..."> " due to an unsanitized file name received from a Content-Disposition header. pacman renames the downloaded package file to match the name given in this header. However, pacman did not sanitize this name, which may contain slashes, before calling rename(). A malicious server (or a network MitM if downloading over HTTP) can send a Content-Disposition header to make pacman place the file anywhere in the filesystem, potentially leading to arbitrary root code execution. Notably, this bypasses pacman's package signature checking. This occurs in curl_download_internal in lib/libalpm/dload.c." />

CVE-2019-9686

Published on: 03/11/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:08 PM UTC

CVE-2019-9686

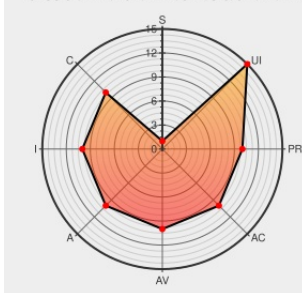
[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Pacman](#) from [Pacman Project](#) contain the following vulnerability:

pacman before 5.1.3 allows directory traversal when installing a remote package via a specified URL "pacman -U <url>" due to an unsanitized file name received from a Content-Disposition header. pacman renames the downloaded package file to match the name given in this header. However, pacman did not sanitize this name, which may

contain slashes, before calling rename(). A malicious server (or a network MitM if downloading over HTTP) can send a Content-Disposition header to make pacman place the file anywhere in the filesystem, potentially leading to arbitrary root code execution. Notably, this bypasses pacman's package signature checking. This occurs in curl_download_internal in lib/libalpm/dload.c.

CVE-2019-9686 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
pacman.git - The official pacman repository	Mailing List Patch Third Party Advisory git.archlinux.org text/html	 MISC git.archlinux.org/pacman.git/commit/?id=9702703633bec2c007730006de2aeeec8587dfc84
pacman.git - The official pacman repository	Mailing List Patch Third Party Advisory git.archlinux.org text/html	 MISC git.archlinux.org/pacman.git/commit/?id=d197d8ab82cf10650487518fb968067897a12775
pacman.git - The official pacman repository	Mailing List Third Party Advisory git.archlinux.org text/html	 MISC git.archlinux.org/pacman.git/commit/?h=release/5.1.x&id=1bf767234363f7ad5933af3f7ce267c123017bde

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

501108 Alpine Linux Security Update for pacman

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pacman Project	Pacman	All	All	All	All
Application	Pacman Project	Pacman	All	All	All	All
cpe:2.3:a:pacman_project:pacman:*****:						
cpe:2.3:a:pacman_project:pacman:*****:						

No vendor comments have been submitted for this CVE

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)