



CVE-2019-11366

Published on: 04/20/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:35 PM UTC

CVE-2019-11366

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H



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

An issue was discovered in atftpd in atftp 0.7.1. It does not lock the thread_list_mutex mutex before assigning the current thread data structure. As a result, the daemon is vulnerable to a denial of service attack due to a NULL pointer dereference. If thread_data is NULL when assigned to current, and modified by another thread before a certain tftpd_list.c check, there is a crash when dereferencing current->next.

CVE-2019-11366 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
USN-4540-1: atftpd vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4540-1

[SECURITY] [DLA 1783-1] atftp security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20190512 [SECURITY] [DLA 1783-1] atftp security update
Debian -- Security Information -- DSA-4438-1 atftp	www.debian.org Deprecated Link text/html	DEBIAN DSA-4438
atftpd - Multiple Memory Corruption Vulnerabilities (CVE-2019-11365, CVE-2019-11366)	Exploit Third Party Advisory pulsesecurity.co.nz text/html	MISC pulsesecurity.co.nz/advisories/atftpd-multiple-vulnerabilities
Bugtraq: [SECURITY] [DSA 4438-1] atftp security update	seclists.org text/html	BUGTRAQ 20190508 [SECURITY] [DSA 4438-1] atftp security update
atftp / Code / Commit [382f76]	Patch Third Party Advisory sourceforge.net text/html	MISC sourceforge.net/p/atftp/code/ci/382f76a90b44f81fec00e2f609a94def4a5d3580/
atftp: Multiple vulnerabilities (GLSA 202003-14) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202003-14

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Atftp Project	Atftp	0.7.1	All	All	All
Application	Atftp Project	Atftp	0.7.1	All	All	All
cpe:2.3:a:atftp_project:atftp:0.7.1:*****:						
cpe:2.3:a:atftp_project:atftp:0.7.1:*****:						

No vendor comments have been submitted for this CVE