

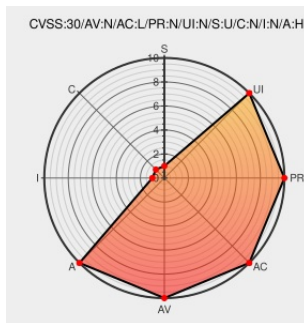


CVE-2017-11746

Published on: 07/30/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:25 PM UTC

CVE-2017-11746

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Tenshi](#) from [Inversepath](#) contain the following vulnerability:

Tenshi 0.15 creates a tenshi.pid file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for tenshi.pid modification before a root script executes a "kill `cat /pathname/tenshi.pid`" command.

CVE-2017-11746 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **7.8 - HIGH**

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

CVE References

Description	Tags	Link
tenshi: Privilege escalation (GLSA 201804-18) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201804-18
Tenshi should create its PID file before dropping privileges (CVE-2017-	Third-Party Advisory	MISC

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

710211 Gentoo Linux tenshi Privilege escalation Vulnerability (GLSA 201804-18)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Inversepath	Tenshi	0.15	All	All	All
Application	Inversepath	Tenshi	0.15	All	All	All
cpe:2.3:a:inversepath:tenshi:0.15:*:*:*:*:*:						
cpe:2.3:a:inversepath:tenshi:0.15:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →