



CVE-2017-7572

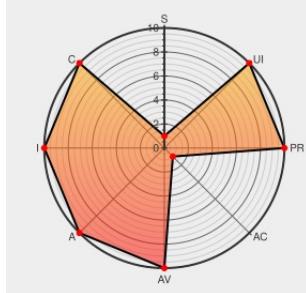
Published on: 04/06/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:41 PM UTC

CVE-2017-7572

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

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



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

The `_checkPolkitPrivilege` function in `serviceHelper.py` in Back In Time (aka backintime) 1.1.18 and earlier uses a deprecated polkit authorization method (`unix-process`) that is subject to a race condition (time of check, time of use). With this authorization method, the owner of a process requesting a polkit operation is checked by polkitd via `/proc/<pid>/status`, by which time the requesting process may have been replaced by a different process with the same PID that has different privileges than the original requester.

CVE-2017-7572 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
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
polkit Check Authorization fix race	CVE-2017-7572	MISC github.com/bit

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	Backintime Project	Backintime	All	All	All	All
cpe:2.3:a:backintime_project:backintime:*****::						

No vendor comments have been submitted for this CVE