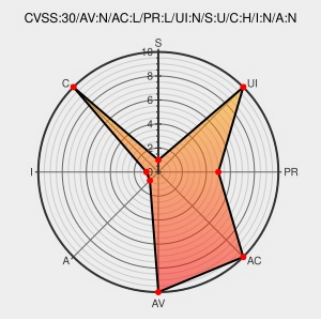
CVE-2017-6200

Published on: 02/06/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:50 PM UTC

CVE-2017-6200

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Sandstorm from Sandstorm contain the following vulnerability:

Sandstorm before build 0.203 allows remote attackers to read any specified file under /etc or /run via the sandbox backup function. The root cause is that the findFilesToZip function doesn't filter Line Feed (\n) characters in a directory name.

CVE-2017-6200 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
sandstorm/backup.c++ at v0.202 · sandstorm-io/sandstorm · GitHub	Third Party Advisory, github.com, text/html	MISC github.com/sandstorm-io/sandstorm/blob/v0.202/src/sandstorm/backup.c%2B%2B#L271
Sandstorm gets a security review -	Vendor Advisory	CONFIRM sandstorm.io/news/2017-03-02-security-review

Sandstorm Blog	sandstorm.io text/html	
Fix newline detection in zip paths. · sandstorm-io/sandstorm@6e8572e · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/sandstorm-io/sandstorm/commit/6e8572ea8bb56d0216bb1b410e5040edc051b120
Improve security of zip/unzip sandbox by switching the sandboxed file… · sandstorm-io/sandstorm@4ea8df7 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/sandstorm-io/sandstorm/commit/4ea8df7403381d9b657b121b3c98d8081b27414d
Sandstorm Security Review | DEVCORE	Exploit Third Party Advisory devco.re text/html	✓ MISC devco.re/blog/2018/01/26/Sandstorm-Security-Review-CVE-2017-6200-en/

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	Sandstorm	Sandstorm	All	All	All	All
Application	Sandstorm	Sandstorm	All	All	All	All

cpe:2.3:a:sandstorm:sandstorm:*:*:*:*:*:*:*:*:

cpe:2.3:a:sandstorm:sandstorm:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→