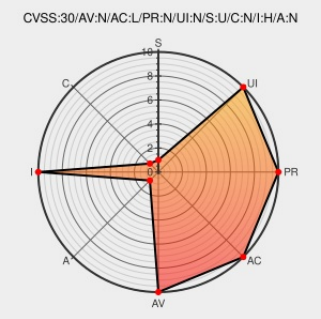
CVE-2018-12088

Published on: 06/10/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:23 PM UTC

CVE-2018-12088

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



Certain versions of S3ql from S3ql Project contain the following vulnerability:

S3QL before 2.27 mishandles checksumming, and consequently allows replay attacks in which an attacker who controls the backend can present old versions of the filesystem metadata database as up-to-date, temporarily inject zero-valued bytes into files, or temporarily hide parts of files. This is related to the checksum_basic_mapping function.

CVE-2018-12088 has been assigned by 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	HIGH	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Repository deleted — Bitbucket	Patch Third Party Advisory bitbucket.org	CONFIRM bitbucket.org/nikratio/s3ql/commits/85aba5c2d5c81453a73a50ed638adaeef0521020

	text/html Inactive Link Not Archived	
Repository deleted — Bitbucket	Exploit Third Party Advisory bitbucket.org text/html Inactive Link Not Archived	CONFIRM bitbucket.org/nikratio/s3ql/issues/272/t3_verifypy-test_retrieve-sometimes-fails
Google Groups	Third Party Advisory groups.google.com text/html	CONFIRM groups.google.com/forum/#!topic/s3ql/4TzCVIMkA4o

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	S3ql Project	S3ql	All	All	All	All
Application	S3ql Project	S3ql	All	All	All	All

cpe:2.3:a:s3ql_project:s3ql:*:*:*:*:*:*:*:*:

cpe:2.3:a:s3ql_project:s3ql:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→