

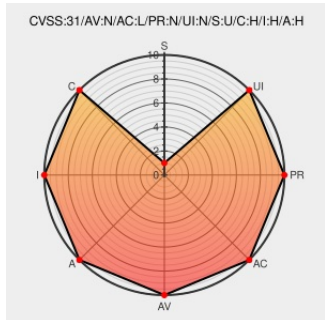


CVE-2021-36372

Published on: 11/19/2021 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:36:00 AM UTC

CVE-2021-36372

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

Certain versions of [Ozone](#) from [Apache](#) contain the following vulnerability:

In Apache Ozone versions prior to 1.2.0, Initially generated block tokens are persisted to the metadata database and can be retrieved with authenticated users with permission to the key. Authenticated users may use them even after access is revoked.

CVE-2021-36372 has been assigned by security@apache.org to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **Apache Software Foundation - Apache Ozone** version <= 1.1

Vulnerability Patch/Work Around

Upgrade to Apache Ozone release version 1.2.0

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link				
oss-security - CVE-2021-36372: Apache Ozone: Original block tokens are persisted and can be retrieved	www.openwall.com text/html	 MLIST [oss-security] 20211118 CVE-2021-36372: Apache Ozone: Original block tokens are persisted and can be retrieved				
CVE-2021-36372: Apache Ozone: Original block tokens are persisted and can be retrieved	mail-archives.apache.org text/xml	 MISC mail-archives.apache.org/mod_mbox/ozone-dev/202111.mbox/%3C5029c1ac-4685-8492-e3cb-ab48c5c370cf%40apache.org%3E				
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	Apache	Ozone	All	All	All	All
cpe:2.3:a:apache:ozone:*****:						
Discovery Credit						
Apache Ozone would like to thank Marton Elek for reporting this issue.						
Social Mentions						
Source	Title					Posted (UTC)
 @CVEreport	CVE-2021-36372 : In #Apache Ozone versions prior to 1.2.0, Initially generated block tokens are persisted to the me... twitter.com/i/web/status/1...					2021-11-19 09:27:42
← Previous ID			Next ID →			