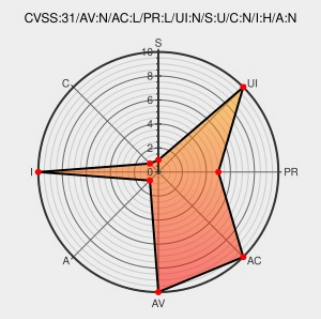
CVE-2018-1000814

Published on: 12/20/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:31 PM UTC

CVE-2018-1000814

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



Certain versions of Aiohttp-session from Aiohttp-session Project contain the following vulnerability:

aio-libs aiohttp-session version 2.6.0 and earlier contains a Other/Unknown vulnerability in EncryptedCookieStorage and NaClCookieStorage that can result in Non-expiring sessions / Infinite lifespan. This attack appear to be exploitable via Recreation of a cookie post-expiry with the same value.

CVE-2018-1000814 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	NONE	HIGH	NONE

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Empty session data if session age > max_age by panagiks · Pull Request #331 · aio-libs/aiohttp-session · GitHub	Patch, Third Party Advisory, github.com	MISC github.com/aio-libs/aiohttp-session/pull/331

	text/html	
Improper Session Expiration in storages with no inherent expiration · Issue #325 · aio-libs/aiohttp-session · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/aio-libs/aiohttp-session/issues/325

Related QID Numbers

980977 Python (pip) Security Update for aiohttp-session (GHSA-mr4x-c4v9-x729)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aiohttp-session Project	Aiohttp-session	All	All	All	All

cpe:2.3:a:aiohttp-session_project:aiohttp-session:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→