eid-login-nextcloud
Code Security Report

7e6034d1-26c8-4f8d-aaae-e0a73182dd33 | 2022-04-20T10:27:38.885Z

Table of Contents

Executive Summary 3

Scan Summary 4

Scan Results 5

- SAST 5
- SCA 7
- KICS 11

Executive Summary

Total Vulnerabilities

Vulnerabilities per Scanner

Scan Information

Project name:	eid-login-nextcloud	
Scanners:	SAST, SCA	
Risk level:	High	
Result triage:	SAST:	
	Urgent	0%
	To verify	0%
	Not exploitable	1400%
	Confirmed	100%
	SCA:	
	Urgent	0%
	To verify	100%
	Not exploitable	0%
	Confirmed	0%

Scan Summary

Scan ID:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Languages:	JavaScript, PHP, JavaScript
Number of scanners:	2
Completed date:	2022-04-06 12:11:03.332084 +0000 UTC
Scanner types:	SAST, SCA

Scan Results

SAST

2 1 1 0 0

JavaScript

Use_Of_Hardcoded_Password (12)

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"testuser993882719"
Source file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Destination node:	password
Destination file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"testuser993882719"
Source file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Destination node:	password
Destination file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"testuser993882719"
Source file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Destination node:	password
Destination file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"testuser993882719"
Source file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Destination node:	password
Destination file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"testuser993882719"
Source file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Destination node:	password
Destination file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"testuser993882719"
Source file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Destination node:	password
Destination file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"testuser993882719"
Source file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Destination node:	password
Destination file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"testuser993882719"
Source file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Destination node:	password
Destination file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"testuser993882719"
Source file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Destination node:	password
Destination file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"testuser993882719"
Source file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Destination node:	password
Destination file:	/eid-login-nextcloud/cypress/integration/personal_settings_login.spec.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"p396ncpass"
Source file:	/eid-login-nextcloud/cypress/plugins/index.js
Destination node:	password
Destination file:	/eid-login-nextcloud/cypress/plugins/index.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	"adminP396"
Source file:	/eid-login-nextcloud/cypress/support/commands.js
Destination node:	pass
Destination file:	/eid-login-nextcloud/cypress/support/commands.js
Compliances:	OWASP Top 10 2021, FISMA 2014, NIST SP 800-53, OWASP Top 10 2017
CWE:	CWE-259

PHP

Use_of_Hard_coded_Cryptographic_Key (4)

NEW

State:	Not exploitable
Status:	NEW
Group name:	PHP_Medium_Threat
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	configKeyCertEnc
Source file:	/eid-login-nextcloud/lib/Service/SslService.php
Compliances:	NIST SP 800-53, OWASP Top 10 2013, OWASP Top 10 2017, OWASP Top 10 2021, PCI DSS v3.2.1, FISMA 2014
CWE:	CWE-321

NEW

State:	Not exploitable
Status:	NEW
Group name:	PHP_Medium_Threat
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	configKeyKeyEnc
Source file:	/eid-login-nextcloud/lib/Service/SslService.php
Compliances:	NIST SP 800-53, OWASP Top 10 2013, OWASP Top 10 2017, OWASP Top 10 2021, PCI DSS v3.2.1, FISMA 2014
CWE:	CWE-321

M NEW

State:	Not exploitable
Status:	NEW
Group name:	PHP_Medium_Threat
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	configKeyCertEnc
Source file:	/eid-login-nextcloud/lib/Service/SslService.php
Compliances:	NIST SP 800-53, OWASP Top 10 2013, OWASP Top 10 2017, OWASP Top 10 2021, PCI DSS v3.2.1, FISMA 2014
CWE:	CWE-321

M NEW

State:	Not exploitable
Status:	NEW
Group name:	PHP_Medium_Threat
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	configKeyKeyEnc
Source file:	/eid-login-nextcloud/lib/Service/SslService.php
Compliances:	NIST SP 800-53, OWASP Top 10 2013, OWASP Top 10 2017, OWASP Top 10 2021, PCI DSS v3.2.1, FISMA 2014
CWE:	CWE-321

JavaScript

Client_DOM_XSS (1)

H NEW

State:	Confirmed
Status:	NEW
Group name:	JavaScript_High_Risk
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	value
Source file:	/eid-login-nextcloud/src/eidlogin-adminsettings.js
Destination node:	innerHTML
Destination file:	/eid-login-nextcloud/src/eidlogin-adminsettings.js
Compliances:	ASD STIG 4.10, FISMA 2014, NIST SP 800-53, OWASP Top 10 2013, OWASP Top 10 2017, OWASP Top 10 2021, PCI DSS v3.2.1
CWE:	CWE-79

Unsafe_Use_Of_Target_blank (12)

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a target="_blank" href="<?php p($faqURL); ?>">
Source file:	/eid-login-nextcloud/templates/personalsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a target="_blank" href="<?php p($tr03130URL)?>">
Source file:	/eid-login-nextcloud/templates/adminsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a target="_blank" href="https://www.ausweisapp.bund.de/ausweisapp2/">>
Source file:	/eid-login-nextcloud/templates/adminsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a target="_blank" href="<?php p($oecURL); ?>">
Source file:	/eid-login-nextcloud/templates/adminsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a target="_blank" href="<?php p($tr03130URL)?>">
Source file:	/eid-login-nextcloud/templates/adminsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a target="_blank" href="<?php p($skidURL); ?>">
Source file:	/eid-login-nextcloud/templates/adminsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a href="<?php p($skidURL); ?>" target="_blank">
Source file:	/eid-login-nextcloud/templates/adminsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a target="_blank" href="https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03130/TR-03130_node.html">
Source file:	/eid-login-nextcloud/templates/adminsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a target="_blank" href="https://sp.skidentity.de/">
Source file:	/eid-login-nextcloud/templates/adminsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a target="_blank" href="<?php p($skidURL); ?>">
Source file:	/eid-login-nextcloud/templates/adminsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a target="_blank" href="https://www.personalausweisportal.de/SharedDocs/faqs/Webs/PA/DE/Haeufige-Fragen/9_pseudonymfunktikon/pseudonymfunktion-liste.html">
Source file:	/eid-login-nextcloud/templates/adminsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	<a target="_blank" href="https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/online-ausweisen/online-ausweisen-node.html">>
Source file:	/eid-login-nextcloud/templates/adminsettings.php
Compliances:	NIST SP 800-53, FISMA 2014
CWE:	CWE-1022

Client_Potential_XSS (1)

NEW

State:	Confirmed
Status:	NEW
Group name:	JavaScript_Medium_Threat
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:09:11 +0000 UTC
First found date:	2022-04-06 12:09:09 +0000 UTC
Source node:	value
Source file:	/eid-login-nextcloud/src/eidlogin-adminsettings.js
Destination node:	innerHTML
Destination file:	/eid-login-nextcloud/src/eidlogin-adminsettings.js
Compliances:	OWASP Top 10 2013, OWASP Top 10 2017, OWASP Top 10 2021, PCI DSS v3.2.1, ASD STIG 4.10, FISMA 2014, NIST SP 800-53
CWE:	CWE-79

SCA

7 5 1 1 0

Vulnerable packages (7)

Npm-yauzl-2.10.0

H NEW | 22

State:	To verify
Status:	NEW
First scan id:	717f911d-ca9d-47d5-b005-9c1cc6306ac7
Found date:	2022-04-06 12:11:01 +0000 UTC
First found date:	2022-03-25 12:42:47 +0000 UTC
Version:	2.10.0
Outdated:	No
CWE:	CWE-22
CVE:	Cxf6e7f2c1-dc59
Description:	The package yauzl is vulnerable to arbitrary file write implemented through improper validation of symlinks. The function validateFileName in the file `index.js` doesn't validate malicious symlink files when checking for path traversal attacks. This affects the integrity & availability.

Npm-nanoid-3.1.30

M NEW | 200

State:	To verify
Status:	NEW
First scan id:	717f911d-ca9d-47d5-b005-9c1cc6306ac7
Found date:	2022-04-06 12:10:59 +0000 UTC
First found date:	2022-03-25 12:42:44 +0000 UTC
Version:	3.1.30
Outdated:	Yes
CWE:	CWE-200
CVE:	CVE-2021-23566
Description:	The package nanoid before 3.1.31 are vulnerable to Information Exposure via the valueOf() function which allows to reproduce the last id generated.

Npm-inflight-1.0.6

NEW | 772

State:	To verify
Status:	NEW
First scan id:	717f911d-ca9d-47d5-b005-9c1cc6306ac7
Found date:	2022-04-06 12:10:59 +0000 UTC
First found date:	2022-03-25 12:42:43 +0000 UTC
Version:	1.0.6
Outdated:	No
CWE:	CWE-772
CVE:	Cxdca8e59f-8bfe
Description:	In npm inflight there is a memory leak because some resources are not freed correctly after being used. It appears to affect all versions.

Npm-debug-3.2.7

NEW | 624

State:	To verify
Status:	NEW
First scan id:	717f911d-ca9d-47d5-b005-9c1cc6306ac7
Found date:	2022-04-06 12:10:59 +0000 UTC
First found date:	2022-03-25 12:42:43 +0000 UTC
Version:	3.2.7
Outdated:	Yes
CWE:	CWE-624
CVE:	Cx8bc4df28-fcf5
Description:	debug accepts a regular expression from user input without escaping it. Arbitrary regular expressions could be injected to cause a denial of service attack on the user's browser.

Npm-debug-3.2.7

NEW | 401

State:	To verify
Status:	NEW
First scan id:	717f911d-ca9d-47d5-b005-9c1cc6306ac7
Found date:	2022-04-06 12:10:59 +0000 UTC
First found date:	2022-03-25 12:42:43 +0000 UTC
Version:	3.2.7
Outdated:	Yes
CWE:	CWE-401
CVE:	Cx89601373-08db
Description:	debug before 4.3.0 has a memory leak when creating debug instances.

Npm-cached-path-relative-1.0.2

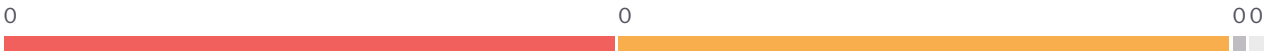
NEW | 1321

State:	To verify
Status:	NEW
First scan id:	10ff2834-9c55-4894-9fb8-9f9fd6f93980
Found date:	2022-04-06 12:10:59 +0000 UTC
First found date:	2022-04-06 12:10:59 +0000 UTC
Version:	1.0.2
Outdated:	Yes
CWE:	CWE-1321
CVE:	CVE-2021-23518
Description:	The package cached-path-relative before 1.1.0 are vulnerable to Prototype Pollution via the cache variable that is set as {} instead of Object.create(null) in the cachedPathRelative function, which allows access to the parent prototype properties when the object is used to create the cached relative path. When using the origin path as __proto__, the attribute of the object is accessed instead of a path. **Note:** This vulnerability derives from an incomplete fix in CVE-2018-16472.

Npm-bluebird-3.7.2

NEW | 401

State:	To verify
Status:	NEW
First scan id:	717f911d-ca9d-47d5-b005-9c1cc6306ac7
Found date:	2022-04-06 12:10:59 +0000 UTC
First found date:	2022-03-25 12:42:43 +0000 UTC
Version:	3.7.2
Outdated:	No
CWE:	CWE-401
CVE:	Cxda14f253-4e52
Description:	The package `bluebird` is vulnerable to memory leak, when running the function longStackTraces() with the flag `--expose_gc`. This causes a significant increase in the memory usage, affecting the server's availability.

KICS

0