eid-login-wordpress
Code Security Report

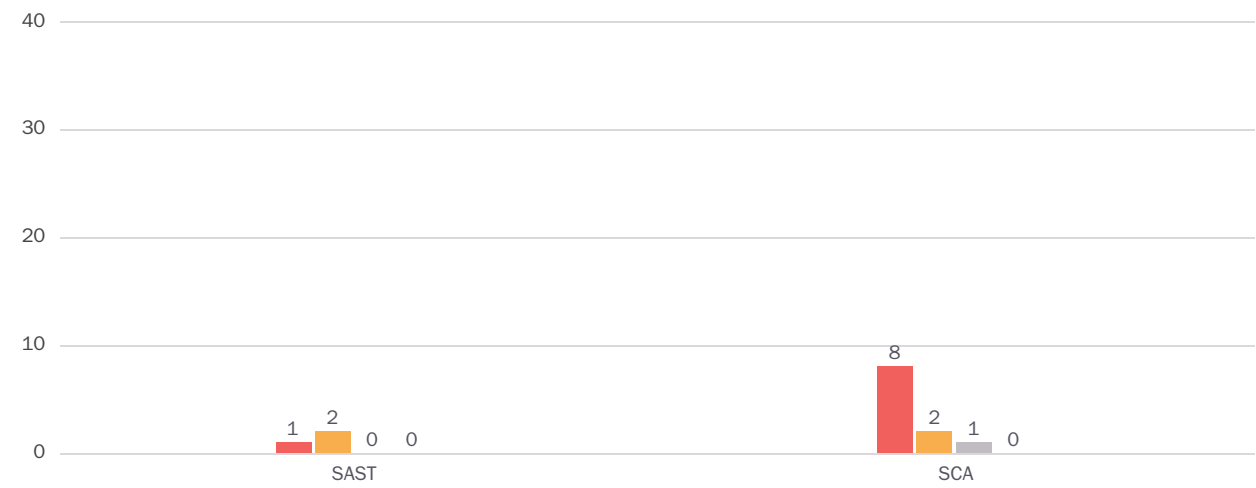
7e6034d1-26c8-4f8d-aaae-e0a73182dd33 | 2022-04-20T10:18:13.288Z

Table of Contents

Executive Summary

Total Vulnerabilities

Vulnerabilities per Scanner



Scan Information

Project name:	eid-login-wordpress	
Scanners:	SAST, SCA	
Risk level:	High	
Result triage:	SAST:	
	To verify	0%
	Not exploitable	566%
	Confirmed	100%
	Urgent	0%
	SCA:	
	Confirmed	0%
	Urgent	0%
	To verify	100%
	Not exploitable	0%

Scan Summary

Scan ID:	87f5f58a-4fca-406c-bf00-6dc18410110f
Languages:	JavaScript, PHP, JavaScript
Number of scanners:	2
Completed date:	2022-04-06 12:26:21.334053 +0000 UTC
Scanner types:	SAST, SCA

SAST

JavaScript

Unsafe_Use_Of_Target_blank (12)

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a id="perso-help" href="https://eid.services/eidlogin/wordpress/userdocs?lang=en" target="_blank">
Source file:	/eid-login-wordpress/tmpl/perso-button.html
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a href="https://eid.services/eidlogin/wordpress/userdocs?lang=en" target="_blank">
Source file:	/eid-login-wordpress/saml/class-eidlogin-saml.php
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a href="https://www.ausweisapp.bund.de/ausweisapp2/" target="_blank">
Source file:	/eid-login-wordpress/includes/class-eidlogin-i18n.php
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a href="https://www.openecard.org/en/download/pc/" target="_blank">
Source file:	/eid-login-wordpress/includes/class-eidlogin-i18n.php
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130_TR-eID-Server_Part1.pdf?__blob=publicationFile&v=1" target="_blank">
Source file:	/eid-login-wordpress/includes/class-eidlogin-i18n.php
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a target="_blank" href="https://skidentity.com">
Source file:	/eid-login-wordpress/includes/class-eidlogin-i18n.php
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a href="https://skidentity.com/" target="_blank">
Source file:	/eid-login-wordpress/includes/class-eidlogin-i18n.php
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a 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" target="_blank">
Source file:	/eid-login-wordpress/includes/class-eidlogin-i18n.php
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a href="https://sp.skidentity.de/" target="_blank">
Source file:	/eid-login-wordpress/includes/class-eidlogin-i18n.php
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a href="https://skidentity.com/" target="_blank">
Source file:	/eid-login-wordpress/includes/class-eidlogin-i18n.php
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a href="https://www.personalausweisportal.de/SharedDocs/faqs/Webs/PA/DE/Haeufige-Fragen/9_pseudonymfunktikon/pseudonymfunktion-liste.html" target="_blank">
Source file:	/eid-login-wordpress/includes/class-eidlogin-i18n.php
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	<a href="https://www.personalausweisportal.de/Webs/PA/EN/citizens/electronic-identification/electronic-identification-node.html" target="_blank">
Source file:	/eid-login-wordpress/includes/class-eidlogin-i18n.php
Compliances:	FISMA 2014, NIST SP 800-53
CWE:	CWE-1022

PHP

Use_Of_Hardcoded_Password (1)

NEW

State:	Not exploitable
Status:	NEW
Group name:	PHP_Low_Visibility
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	"true"
Source file:	/eid-login-wordpress/saml/class-eidlogin-saml.php
Compliances:	NIST SP 800-53, OWASP Top 10 2013, OWASP Top 10 2017, OWASP Top 10 2021, PCI DSS v3.2.1, ASD STIG 4.10, FISMA 2014
CWE:	CWE-259

CSRF (1)

NEW

State:	Confirmed
Status:	NEW
Group name:	PHP_Medium_Threat
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	_GET
Source file:	/eid-login-wordpress/saml/class-eidlogin-saml.php
Destination node:	query
Destination file:	/eid-login-wordpress/db/class-eidlogin-response-data.php
Compliances:	PCI DSS v3.2.1, ASD STIG 4.10, NIST SP 800-53, OWASP Top 10 2013, OWASP Top 10 2021
CWE:	CWE-352

JavaScript

Use_Of_Hardcoded_Password (4)

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	"testuser123"
Source file:	/eid-login-wordpress/cypress/integration/skidentity.spec.js
Destination node:	password
Destination file:	/eid-login-wordpress/cypress/integration/skidentity.spec.js
Compliances:	OWASP Top 10 2017, OWASP Top 10 2021, FISMA 2014, NIST SP 800-53
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	"testuser123"
Source file:	/eid-login-wordpress/cypress/integration/skidentity.spec.js
Destination node:	password
Destination file:	/eid-login-wordpress/cypress/integration/skidentity.spec.js
Compliances:	OWASP Top 10 2017, OWASP Top 10 2021, FISMA 2014, NIST SP 800-53
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	"p396wppass"
Source file:	/eid-login-wordpress/cypress/plugins/index.js
Destination node:	password
Destination file:	/eid-login-wordpress/cypress/plugins/index.js
Compliances:	OWASP Top 10 2017, OWASP Top 10 2021, FISMA 2014, NIST SP 800-53
CWE:	CWE-259

NEW

State:	Not exploitable
Status:	NEW
Group name:	JavaScript_Server_Side_Vulnerabilities
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	"testuser123"
Source file:	/eid-login-wordpress/cypress/support/commands.js
Destination node:	default_password
Destination file:	/eid-login-wordpress/cypress/support/commands.js
Compliances:	OWASP Top 10 2017, OWASP Top 10 2021, FISMA 2014, NIST SP 800-53
CWE:	CWE-259

Client_DOM_XSS (1)

NEW

State:	Confirmed
Status:	NEW
Group name:	JavaScript_High_Risk
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	value
Source file:	/eid-login-wordpress/admin/js/eidlogin-admin.js
Destination node:	innerHTML
Destination file:	/eid-login-wordpress/admin/js/eidlogin-admin.js
Compliances:	OWASP Top 10 2021, PCI DSS v3.2.1, ASD STIG 4.10, FISMA 2014, NIST SP 800-53, OWASP Top 10 2013, OWASP Top 10 2017
CWE:	CWE-79

Client_Potential_XSS (1)

NEW

State:	Confirmed
Status:	NEW
Group name:	JavaScript_Medium_Threat
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:09:56 +0000 UTC
First found date:	2022-04-06 12:09:54 +0000 UTC
Source node:	value
Source file:	/eid-login-wordpress/admin/js/eidlogin-admin.js
Destination node:	innerHTML
Destination file:	/eid-login-wordpress/admin/js/eidlogin-admin.js
Compliances:	OWASP Top 10 2017, OWASP Top 10 2021, PCI DSS v3.2.1, ASD STIG 4.10, FISMA 2014, NIST SP 800-53, OWASP Top 10 2013
CWE:	CWE-79

SCA

11

Vulnerable packages (11)

Composer-twig/twig-v3.3.2

NEW | 74

State:	To verify
Status:	NEW
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:10:50 +0000 UTC
First found date:	2022-04-06 12:10:50 +0000 UTC
Version:	v3.3.2
Outdated:	Yes
CWE:	CWE-74
CVE:	CVE-2022-23614
Description:	Twig is an open source template language for PHP. In Twig versions 2.0.x before 2.14.11, 3.0.x before 3.3.8 when in a sandbox mode, the `arrow` parameter of the `sort` filter must be a closure to avoid attackers being able to run arbitrary PHP functions. In affected versions this constraint was not properly enforced and could lead to code injection of arbitrary PHP code. Patched versions now disallow calling non Closure in the `sort` filter as is the case for some other filters. Users are advised to upgrade.

Npm-yauzl-2.10.0

NEW | 22

State:	To verify
Status:	NEW
First scan id:	717f911d-ca9d-47d5-b005-9c1cc6306ac7
Found date:	2022-04-06 12:10:48 +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-json-schema-0.2.3

NEW | 1321

State:	To verify
Status:	NEW
First scan id:	717f911d-ca9d-47d5-b005-9c1cc6306ac7
Found date:	2022-04-06 12:10:48 +0000 UTC
First found date:	2022-03-25 12:42:44 +0000 UTC
Version:	0.2.3
Outdated:	Yes
CWE:	CWE-1321
CVE:	CVE-2021-3918
Description:	json-schema before 0.4.0 is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

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 12:10:48 +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-4.3.2

NEW | 624

State:	To verify
Status:	NEW
First scan id:	717f911d-ca9d-47d5-b005-9c1cc6306ac7
Found date:	2022-04-06 12:10:48 +0000 UTC
First found date:	2022-03-25 12:42:43 +0000 UTC
Version:	4.3.2
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-3.2.6

NEW | 401

State:	To verify
Status:	NEW
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:10:48 +0000 UTC
First found date:	2022-04-06 12:10:48 +0000 UTC
Version:	3.2.6
Outdated:	Yes
CWE:	CWE-401
CVE:	Cx65603961-769c
Description:	The package debug is vulnerable to memory leakage when instance is created inside a function. The function `debug` in the file `common.js` does not free up used memory unless there's a call to `destroy()` function. This affects the availability.

Npm-debug-3.2.6

NEW | 400

State:	To verify
Status:	NEW
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:10:48 +0000 UTC
First found date:	2022-04-06 12:10:48 +0000 UTC
Version:	3.2.6
Outdated:	Yes
CWE:	CWE-400
CVE:	Cxbd6f2b91-dd38
Description:	The debug module is vulnerable to regular expression denial of service when untrusted user input is passed into the o formatter. It takes around 50k characters to block for 2 seconds making this a low severity issue. This vulnerability is a reintroduction of CVE-2017-16137 in version 3.2.0.

Npm-debug-3.2.6

NEW | 401

State:	To verify
Status:	NEW
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:10:48 +0000 UTC
First found date:	2022-04-06 12:10:48 +0000 UTC
Version:	3.2.6
Outdated:	Yes
CWE:	CWE-401
CVE:	Cx89601373-08db
Description:	debug before 4.3.0 has a memory leak when creating debug instances.

Npm-debug-3.2.6

NEW | 624

State:	To verify
Status:	NEW
First scan id:	87f5f58a-4fca-406c-bf00-6dc18410110f
Found date:	2022-04-06 12:10:48 +0000 UTC
First found date:	2022-04-06 12:10:48 +0000 UTC
Version:	3.2.6
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-bluebird-3.7.2

NEW | 401

State:	To verify
Status:	NEW
First scan id:	717f911d-ca9d-47d5-b005-9c1cc6306ac7
Found date:	2022-04-06 12:10:48 +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.

Npm-ansi-regex-5.0.0

NEW | 1333

State:	To verify
Status:	NEW
First scan id:	717f911d-ca9d-47d5-b005-9c1cc6306ac7
Found date:	2022-04-06 12:10:48 +0000 UTC
First found date:	2022-03-25 12:42:42 +0000 UTC
Version:	5.0.0
Outdated:	Yes
CWE:	CWE-1333
CVE:	CVE-2021-3807
Description:	ansi-regex prior to 5.0.1 and 6.0.x prior to 6.0.1 is vulnerable to Inefficient Regular Expression Complexity

KICS