National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

01 - 15 Jan 2023 Vol. 10 No. 01

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: ays-pro					
Product: survey_maker					
Affected Version(s): * Up to (including) 3.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2023	6.1	The "Survey Maker – Best WordPress Survey Plugin" plugin for WordPress is vulnerable to Stored Cross-Site Scripting via survey answers in versions up to, and including, 3.1.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts when submitting quizzes that will execute whenever a user accesses the submissions page. **CVE ID : CVE-2023-0038**	N/A	A-AYS-SURV-230123/1
Vendor: bzip2_project					
Product: bzip2					
Affected Version(s): * Up to (excluding) 0.4.4					
Integer Overflow or Wraparound	10-Jan-2023	7.5	The bzip2 crate before 0.4.4 for Rust allow attackers to cause a denial of service via a large file that triggers an integer overflow in mem.rs. NOTE: this is unrelated to the https://crates.io/crates/bzip2-rs product.	https://crates.io/crates/bzip2/versions, https://github.com/alexcrichton/bzip2-rs/pull/86	A-BZI-BZIP-230123/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22895		
Vendor: circl					
Product: pandora					
Affected Version(s): * Up to (excluding) 1.3.1					
Improper Input Validation	10-Jan-2023	6.5	workers/extractor.py in Pandora (aka pandora-analysis/pandora) 1.3.0 allows a denial of service when an attacker submits a deeply nested ZIP archive (aka ZIP bomb). **CVE ID : CVE-2023-22898**	https://github.com/pandora-analysis/pandora/commit/1dc06327fdc07c56eae653e497dd137ec70d8265	A-CIR-PAND-230123/3
Vendor: control_id_panel_project					
Product: control_id_panel					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2023	6.1	A vulnerability was found in Control iD Panel. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Web Interface. The manipulation of the argument Nome leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-217717 was assigned to this vulnerability. **CVE ID : CVE-2023-0125**	N/A	A-CON-CONT-230123/4
Vendor: crocoblock					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: jetwidgets_for_elementor					
Affected Version(s): * Up to (including) 1.0.12					
Cross-Site Request Forgery (CSRF)	05-Jan-2023	6.5	The JetWidgets for Elementor plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.12. This is due to missing nonce validation on the save() function. This makes it possible for unauthenticated attackers to to modify the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This can be used to enable SVG uploads that could make Cross-Site Scripting possible. **CVE ID : CVE-2023-0086**	https://plugins.trac.wordpress.org/browser/jetwidgets-for-elementor/trunk/includes/class-jet-widgets-settings.php#L149	A-CRO-JETW-230123/5
Vendor: daloradius					
Product: daloradius					
Affected Version(s): * Up to (excluding) 2023-01-04					
Improper Control of Generation of Code ('Code Injection')	04-Jan-2023	8.8	Code Injection in GitHub repository lirantal/daloradius prior to master-branch. **CVE ID : CVE-2023-0048**	https://huntr.dev/bounties/57abd666-4b9c-4f59-825d-1ec832153e79, https://github.com/lirantal/daloradius/commit/3650eea7277a5c278063	A-DAL-DALO-230123/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				214a5b71dbd7d77fc5aa	
Improper Restriction of Names for Files and Other Resources	04-Jan-2023	7.2	Improper Restriction of Names for Files and Other Resources in GitHub repository lirantal/daloradius prior to master-branch. **CVE ID : CVE-2023-0046**	https://github.com/lirantal/daloradius/commit/2013c2d1231e99dac918247b69b198ded1f30a1c, https://huntr.dev/bounties/2214dc41-f283-4342-95b1-34a2f4fea943	A-DAL-DALO-230123/7
Vendor: discourse					
Product: discourse					
Affected Version(s): * Up to (excluding) 2.8.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/9
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**		
Affected Version(s): 1.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/11
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**		
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/13
Affected Version(s): 1.2.0					
Improper Neutralization of Input During Web Page Generation	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed`	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48	A-DIS-DISC-230123/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	d68a8993a12	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/16
Affected Version(s): 1.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/18
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**		
Affected Version(s): 1.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/20
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**		
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/22
Affected Version(s): 1.5.0					
Improper Neutralization of Input During Web Page Generation	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed`	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48	A-DIS-DISC-230123/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	d68a8993a12	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/25
Affected Version(s): 1.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/27
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**		
Affected Version(s): 1.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/29
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**		
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/31
Affected Version(s): 1.8.0					
Improper Neutralization of Input During Web Page Generation	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed`	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48	A-DIS-DISC-230123/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	d68a8993a12	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/34
Affected Version(s): 1.9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/36
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**		
Affected Version(s): 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/38
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**		
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/40
Affected Version(s): 2.1.0					
Improper Neutralization of Input During Web Page Generation	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed`	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48	A-DIS-DISC-230123/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	d68a8993a12	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/43
Affected Version(s): 2.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/45
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**		
Affected Version(s): 2.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/47
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**		
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/49
Affected Version(s): 2.4.0					
Improper Neutralization of Input During Web Page Generation	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed`	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48	A-DIS-DISC-230123/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	d68a8993a12	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/52
Affected Version(s): 2.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/54
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**		
Affected Version(s): 2.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/56
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**		
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/58
Affected Version(s): 2.7.0					
Improper Neutralization of Input During Web Page Generation	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed`	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48	A-DIS-DISC-230123/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	d68a8993a12	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/61
Affected Version(s): 2.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/63
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**		
Affected Version(s): 2.9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48d68a8993a12	A-DIS-DISC-230123/65
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**		
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/67
Affected Version(s): 3.0.0					
Improper Neutralization of Input During Web Page Generation	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed`	https://github.com/discourse/discourse/commit/c0e2d7badac276d82a4056a994b48	A-DIS-DISC-230123/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16. **CVE ID : CVE-2023-22454**	d68a8993a12	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	6.1	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch. **CVE ID : CVE-2023-22455**	https://github.com/discourse/discourse/commit/692329896ac64d8581947e977202c243eef3b5a2	A-DIS-DISC-230123/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	05-Jan-2023	5.3	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround. **CVE ID : CVE-2023-22453**	https://github.com/discourse/discourse/commit/cbcf8a064b4889a19c991641e09c399bfa1ef2ad	A-DIS-DISC-230123/70
Vendor: fit2cloud					
Product: kubepi					
Affected Version(s): * Up to (excluding) 1.6.3					
Use of Hard-coded Credentials	04-Jan-2023	9.8	KubePi is a k8s panel. The jwt authentication function of KubePi through version 1.6.2 uses hard-coded Jwtsigkeys, resulting in the same Jwtsigkeys for all online projects. This means that an attacker can forge any jwt token to take over the administrator account of any online project. Furthermore, they may use the administrator to take over the k8s cluster of the target enterprise. `session.go`, the use of hard-coded JwtSigKey,	https://github.com/KubeOperator/KubePi/commit/3be58b8df5bc05d2343c30371dd5fcf6a9fbbf8b, https://github.com/KubeOperator/KubePi/security/advisories/GHSA-vjhf-8vqx-vqpq	A-FIT-KUBE-230123/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an attacker to use this value to forge jwt tokens arbitrarily. The JwtSigKey is confidential and should not be hard-coded in the code. The vulnerability has been fixed in 1.6.3. In the patch, JWT key is specified in app.yml. If the user leaves it blank, a random key will be used. There are no workarounds aside from upgrading. **CVE ID : CVE-2023-22463**		
Affected Version(s): * Up to (excluding) 1.6.4					
Session Fixation	10-Jan-2023	6.5	KubePi is a modern Kubernetes panel. A session fixation attack allows an attacker to hijack a legitimate user session, versions 1.6.3 and below are susceptible. A patch will be released in version 1.6.4. **CVE ID : CVE-2023-22479**	https://github.com/KubeOperator/KubePi/security/advisories/GHSA-v4w5-r2xc-7f8h	A-FIT-KUBE-230123/72
Vendor: ftp_project					
Product: ftp					
Affected Version(s): * Up to (including) 2012-03-28					
N/A	01-Jan-2023	7.5	The FTP (aka "Implementation of a simple FTP client and server") project through 96c1a35 allows remote attackers to cause a denial of service (memory consumption)	N/A	A-FTP-FTP-230123/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by engaging in client activity, such as establishing and then terminating a connection. This occurs because malloc is used but free is not. **CVE ID : CVE-2023-22551**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 109.0.5414.74					
Use After Free	10-Jan-2023	8.8	Use after free in Overview Mode in Google Chrome on Chrome OS prior to 109.0.5414.74 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0128**	https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	A-GOO-CHRO-230123/74
Out-of-bounds Write	10-Jan-2023	8.8	Heap buffer overflow in Network Service in Google Chrome prior to 109.0.5414.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page and specific interactions. (Chromium security severity: High)	https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	A-GOO-CHRO-230123/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0129		
Use After Free	10-Jan-2023	8.8	Use after free in Cart in Google Chrome prior to 109.0.5414.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via database corruption and a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-0134**	https://crbug.com/1385709, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	A-GOO-CHRO-230123/76
Use After Free	10-Jan-2023	8.8	Use after free in Cart in Google Chrome prior to 109.0.5414.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via database corruption and a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-0135**	https://crbug.com/1385831, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	A-GOO-CHRO-230123/77
N/A	10-Jan-2023	8.8	Inappropriate implementation in in Fullscreen API in Google Chrome on Android prior to 109.0.5414.74 allowed a remote attacker to execute incorrect security UI via a crafted HTML page. (Chromium security severity: Medium)	https://crbug.com/1356987, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	A-GOO-CHRO-230123/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0136		
Out-of-bounds Write	10-Jan-2023	8.8	Heap buffer overflow in Platform Apps in Google Chrome on Chrome OS prior to 109.0.5414.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-0137**	https://crbug.com/1399904, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	A-GOO-CHRO-230123/79
Out-of-bounds Write	10-Jan-2023	8.8	Heap buffer overflow in libphonenumber in Google Chrome prior to 109.0.5414.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-0138**	https://crbug.com/1346675, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	A-GOO-CHRO-230123/80
N/A	10-Jan-2023	6.5	Inappropriate implementation in in Permission prompts in Google Chrome on Windows prior to 109.0.5414.74 allowed a remote attacker to force acceptance of a permission prompt via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-0132**	https://crbug.com/1371215, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	A-GOO-CHRO-230123/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Jan-2023	6.5	Inappropriate implementation in in Permission prompts in Google Chrome on Android prior to 109.0.5414.74 allowed a remote attacker to bypass main origin permission delegation via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-0133**	https://crbug.com/1375132, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	A-GOO-CHRO-230123/82
N/A	10-Jan-2023	6.5	Inappropriate implementation in in File System API in Google Chrome on Windows prior to 109.0.5414.74 allowed a remote attacker to bypass file system restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-0140**	https://crbug.com/1326788, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	A-GOO-CHRO-230123/83
N/A	10-Jan-2023	4.3	Insufficient policy enforcement in CORS in Google Chrome prior to 109.0.5414.74 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-0141**	https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html, https://crbug.com/1362331	A-GOO-CHRO-230123/84
Affected Version(s): * Up to (excluding) 109.05414.74					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	10-Jan-2023	6.5	Insufficient validation of untrusted input in Downloads in Google Chrome on Windows prior to 109.0.5414.74 allowed a remote attacker to bypass download restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-0139**	https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html, https://crbug.com/1367632	A-GOO-CHRO-230123/85
Vendor: kenny2automate_project					
Product: kenny2automate					
Affected Version(s): * Up to (excluding) a947d7c					
Improper Input Validation	02-Jan-2023	6.5	kenny2automate is a Discord bot. In the web interface for server settings, form elements were generated with Discord channel IDs as part of input names. Prior to commit a947d7c, no validation was performed to ensure that the channel IDs submitted actually belonged to the server being configured. Thus anyone who has access to the channel ID they wish to change settings for and the server settings panel for any server could change settings for the requested channel no matter which server it belonged to. Commit a947d7c resolves the issue and has been	https://github.com/Kenny2github/kenny2automate/commit/a947d7ce408687b587c7e6dfd6026f7c4ee31ac2, https://github.com/Kenny2github/kenny2automate/security/advisories/GHSA-73j8-xrcr-q6j7	A-KEN-KENN-230123/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deployed to the official instance of the bot. The only workaround that exists is to disable the web config entirely by changing it to run on localhost. Note that a workaround is only necessary for those who run their own instance of the bot. **CVE ID : CVE-2023-22452**		
Vendor: kiwitcms					
Product: kiwi_tcms					
Affected Version(s): * Up to (excluding) 11.7					
Weak Password Requirements	02-Jan-2023	8.8	Kiwi TCMS is an open source test management system. In version 11.6 and prior, when users register new accounts and/or change passwords, there is no validation in place which would prevent them from picking an easy to guess password. This issue is resolved by providing defaults for the `AUTH_PASSWORD_VALIDATORS` configuration setting. As of version 11.7, the password can't be too similar to other personal information, must contain at least 10 characters, can't be a commonly used password, and can't be entirely numeric. As a workaround, an administrator may reset	https://huntr.dev/bounties/32a873c8-f605-4aae-9272-d80985ef2b73, https://github.com/kiwitcms/Kiwi/commit/3759fb68aed36315cdde9fc573b2fe7c11544985	A-KIW-KIWI-230123/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all passwords in Kiwi TCMS if they think a weak password may have been chosen. **CVE ID : CVE-2023-22451**		
Vendor: librephotos_project					
Product: librephotos					
Affected Version(s): * Up to (excluding) 2023-01-09					
N/A	10-Jan-2023	9.8	api/views/user.py in LibrePhotos before e19e539 has incorrect access control. **CVE ID : CVE-2023-22903**	https://github.com/LibrePhotos/librephotos/commit/e19e539356df77f6f59e7d1eea22d452b268e120	A-LIB-LIBR-230123/88
Vendor: linagora					
Product: twake					
Affected Version(s): * Up to (including) 2022.q4.1120					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jan-2023	6.1	Cross-site Scripting (XSS) - Stored in GitHub repository linagora/twake prior to 2023.Q1.1200+. **CVE ID : CVE-2023-0028**	https://huntr.dev/bounties/bfd935f4-2d1d-4d3f-8b59-522abe7dd065, https://github.com/linagora/twake/commit/61f4c0caf4ce61c839fb304a707972974daacae9	A-LIN-TWAK-230123/89
Vendor: machothemes					
Product: cpo_companion					
Affected Version(s): * Up to (including) 1.0.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	4.8	The CPO Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of its content type settings parameters in versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-0162**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2844012%40cpo-companion%2Ftrunk&old=2574013%40cpo-companion%2Ftrunk&sfp_email=&sfph_mail=	A-MAC-CPO_-230123/90
Vendor: Mediawiki					
Product: mediawiki					
Affected Version(s): * Up to (excluding) 1.35.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. E-Widgets does widget replacement in HTML attributes, which can lead to XSS, because widget authors often do not expect that their widget is executed in an HTML attribute context. **CVE ID : CVE-2023-22911**	https://phabricator.wikimedia.org/T149488	A-MED-MEDI-230123/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Jan-2023	5.3	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. SpecialMobileHistory allows remote attackers to cause a denial of service because database queries are slow. **CVE ID : CVE-2023-22909**	https://phabricator.wikimedia.org/T320987	A-MED-MEDI-230123/92
Affected Version(s): 1.39.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. E-Widgets does widget replacement in HTML attributes, which can lead to XSS, because widget authors often do not expect that their widget is executed in an HTML attribute context. **CVE ID : CVE-2023-22911**	https://phabricator.wikimedia.org/T149488	A-MED-MEDI-230123/93
N/A	10-Jan-2023	5.3	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. SpecialMobileHistory allows remote attackers to cause a denial of service because database queries are slow. **CVE ID : CVE-2023-22909**	https://phabricator.wikimedia.org/T320987	A-MED-MEDI-230123/94
Affected Version(s): From (including) 1.36.0 Up to (excluding) 1.38.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. E-Widgets does widget replacement in HTML attributes, which can lead to XSS, because widget authors often do not expect that their widget is executed in an HTML attribute context. **CVE ID : CVE-2023-22911**	https://phabricator.wikimedia.org/T149488	A-MED-MEDI-230123/95
N/A	10-Jan-2023	5.3	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. SpecialMobileHistory allows remote attackers to cause a denial of service because database queries are slow. **CVE ID : CVE-2023-22909**	https://phabricator.wikimedia.org/T320987	A-MED-MEDI-230123/96
Vendor: mercurius_project					
Product: mercurius					
Affected Version(s): * Up to (excluding) 8.13.2					
N/A	09-Jan-2023	7.5	Mercurius is a GraphQL adapter for Fastify. Any users of Mercurius until version 10.5.0 are subjected to a denial of service attack by sending a malformed packet over WebSocket to `/graphql`. This issue was patched in #940. As a workaround,	https://github.com/mercurius-js/mercurius/security/advisories/GHSA-cm8h-q92v-xcfc, https://github.com/mercurius-	A-MER-MERC-230123/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users can disable subscriptions. **CVE ID : CVE-2023-22477**	js/mercurius/pull/940	
Affected Version(s): From (including) 9.0.0 Up to (excluding) 11.5.0					
N/A	09-Jan-2023	7.5	Mercurius is a GraphQL adapter for Fastify. Any users of Mercurius until version 10.5.0 are subjected to a denial of service attack by sending a malformed packet over WebSocket to `/graphql`. This issue was patched in #940. As a workaround, users can disable subscriptions. **CVE ID : CVE-2023-22477**	https://github.com/mercurius-js/mercurius/security/advisories/GHSA-cm8h-q92v-xcfc, https://github.com/mercurius-js/mercurius/pull/940	A-MER-MERC-230123/98
Vendor: Microsoft					
Product: 3d_builder					
Affected Version(s): -					
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21781, CVE-2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-2023-21791, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21780**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21780	A-MIC-3D_B-230123/99
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780,	https://portal.msrc.microsoft.com/en-	A-MIC-3D_B-230123/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE-2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-2023-21791, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21781**	US/security-guidance/advisory/CVE-2023-21781	
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-2023-21791, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21782**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21782	A-MIC-3D_B-230123/101
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-2023-21782, CVE-2023-21784, CVE-2023-21785, CVE-2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-2023-21791, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21783**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21783	A-MIC-3D_B-230123/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-2023-21782, CVE-2023-21783, CVE-2023-21785, CVE-2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-2023-21791, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21784**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21784	A-MIC-3D_B-230123/103
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-2023-21791, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21785**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21785	A-MIC-3D_B-230123/104
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21786	A-MIC-3D_B-230123/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-21791, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21786**		
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-2023-21786, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-2023-21791, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21787**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21787	A-MIC-3D_B-230123/106
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-2023-21786, CVE-2023-21787, CVE-2023-21789, CVE-2023-21790, CVE-2023-21791, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21788**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21788	A-MIC-3D_B-230123/107
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21789	A-MIC-3D_B-230123/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21790, CVE-2023-21791, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21789**		
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21791, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21790**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21790	A-MIC-3D_B-230123/109
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-2023-21792, CVE-2023-21793. **CVE ID : CVE-2023-21791**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21791	A-MIC-3D_B-230123/110
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-3D_B-230123/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-2023-21791, CVE-2023-21793. **CVE ID : CVE-2023-21792**	guidance/advisory/CVE-2023-21792	
N/A	10-Jan-2023	7.8	3D Builder Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2023-21780, CVE-2023-21781, CVE-2023-21782, CVE-2023-21783, CVE-2023-21784, CVE-2023-21785, CVE-2023-21786, CVE-2023-21787, CVE-2023-21788, CVE-2023-21789, CVE-2023-21790, CVE-2023-21791, CVE-2023-21792. **CVE ID : CVE-2023-21793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21793	A-MIC-3D_B-230123/112
Vendor: momentjs					
Product: luxon					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.38.1					
N/A	04-Jan-2023	7.5	Luxon is a library for working with dates and times in JavaScript. On the 1.x branch prior to 1.38.1, the 2.x branch prior to 2.5.2, and the 3.x branch on 3.2.1, Luxon's `DateTime.fromRFC2822() has quadratic (N^2) complexity on some specific inputs. This causes a noticeable slowdown for inputs with lengths above 10k	https://github.com/moment/moment/pull/6015#issuecomment-1152961973, https://github.com/moment/luxon/commit/5ab3bf64a10da929a437629	A-MOM-LUXO-230123/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			characters. Users providing untrusted data to this method are therefore vulnerable to (Re)DoS attacks. This issue also appears in Moment as CVE-2022-31129. Versions 1.38.1, 2.5.2, and 3.2.1 contain patches for this issue. As a workaround, limit the length of the input. **CVE ID : CVE-2023-22467**	cdb2f059bb83212bf	
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.5.2					
N/A	04-Jan-2023	7.5	Luxon is a library for working with dates and times in JavaScript. On the 1.x branch prior to 1.38.1, the 2.x branch prior to 2.5.2, and the 3.x branch on 3.2.1, Luxon's `DateTime.fromRFC2822() has quadratic (N^2) complexity on some specific inputs. This causes a noticeable slowdown for inputs with lengths above 10k characters. Users providing untrusted data to this method are therefore vulnerable to (Re)DoS attacks. This issue also appears in Moment as CVE-2022-31129. Versions 1.38.1, 2.5.2, and 3.2.1 contain patches for this issue. As a workaround, limit the length of the input.	https://github.com/moment/moment/pull/6015#issuecomment-1152961973, https://github.com/moment/luxon/commit/5ab3bf64a10da929a437629cdb2f059bb83212bf	A-MOM-LUXO-230123/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22467		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.2.1					
N/A	04-Jan-2023	7.5	Luxon is a library for working with dates and times in JavaScript. On the 1.x branch prior to 1.38.1, the 2.x branch prior to 2.5.2, and the 3.x branch on 3.2.1, Luxon's `DateTime.fromRFC2822() has quadratic (N^2) complexity on some specific inputs. This causes a noticeable slowdown for inputs with lengths above 10k characters. Users providing untrusted data to this method are therefore vulnerable to (Re)DoS attacks. This issue also appears in Moment as CVE-2022-31129. Versions 1.38.1, 2.5.2, and 3.2.1 contain patches for this issue. As a workaround, limit the length of the input. **CVE ID : CVE-2023-22467**	https://github.com/moment/moment/pull/6015#issuecomment-1152961973, https://github.com/moment/luxon/commit/5ab3bf64a10da929a437629cdb2f059bb83212bf	A-MOM-LUXO-230123/115
Vendor: Nextcloud					
Product: deck					
Affected Version(s): * Up to (excluding) 1.8.2					
Insecure Storage of Sensitive Information	10-Jan-2023	3.5	Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. When getting the reference preview for Deck cards the user has	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8fjp-w9gp-	A-NEX-DECK-230123/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no access to, unauthorized user could eventually get the cached data of a user that has access. There are currently no known workarounds. It is recommended that the Nextcloud app Deck is upgraded to 1.8.2. **CVE ID : CVE-2023-22469**	j5hq, https://github.com/nextcloud/deck/pull/4196	
Product: desktop					
Affected Version(s): 3.6.1					
Cross-Site Request Forgery (CSRF)	09-Jan-2023	8.8	Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. It is possible to make a user send any POST request with an arbitrary body given they click on a malicious deep link on a Windows computer. (e.g. in an email, chat link, etc). There are currently no known workarounds. It is recommended that the Nextcloud Desktop client is upgraded to 3.6.2. **CVE ID : CVE-2023-22472**	https://github.com/nextcloud/desktop/pull/5106	A-NEX-DESK-230123/117
Product: talk					
Affected Version(s): * Up to (excluding) 15.0.2					
Improper Access Control	09-Jan-2023	2.1	Talk-Android enables users to have video & audio calls through Nextcloud on Android. Due to passcode bypass,	https://github.com/nextcloud/talk-android/pull/2598	A-NEX-TALK-230123/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attacker is able to access the user's Nextcloud files and view conversations. To exploit this the attacker needs to have physical access to the target's device. There are currently no known workarounds available. It is recommended that the Nextcloud Talk Android app is upgraded to 15.0.2. **CVE ID : CVE-2023-22473**		
Vendor: NSA					
Product: ghidra					
Affected Version(s): * Up to (including) 10.2.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Jan-2023	9.8	Ghidra/RuntimeScripts/Linux/support/launch.sh in NSA Ghidra through 10.2.2 passes user-provided input into eval, leading to command injection when calling analyzeHeadless with untrusted input. **CVE ID : CVE-2023-22671**	https://github.com/NationalSecurityAgency/ghidra/pull/4872	A-NSA-GHID-230123/119
Vendor: odude					
Product: user_post_gallery					
Affected Version(s): * Up to (including) 2.19					
Improper Neutralization of Special Elements used in a Command ('Comman	03-Jan-2023	9.8	The User Post Gallery - UPG plugin for WordPress is vulnerable to authorization bypass which leads to remote command execution due to the use of a nopriv AJAX action and user supplied function calls	N/A	A-ODU-USER-230123/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			and parameters in versions up to, and including 2.19. This makes it possible for unauthenticated attackers to call arbitrary PHP functions and perform actions like adding new files that can be webshells and updating the site's options to allow anyone to register as an administrator. **CVE ID : CVE-2023-0039**		
Vendor: openam					
Product: openam					
Affected Version(s): 4.1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jan-2023	7.5	OpenAM Web Policy Agent (OpenAM Consortium Edition) provided by OpenAM Consortium parses URLs improperly, leading to a path traversal vulnerability(CWE-22). Furthermore, a crafted URL may be evaluated incorrectly. **CVE ID : CVE-2023-22320**	https://github.com/openam-jp/web-agents/issues/3	A-OPE-OPEN-230123/121
Vendor: openharmony					
Product: openharmony					
Affected Version(s): From (including) 3.0 Up to (including) 3.0.5					
Authentication Bypass by Capture-replay	09-Jan-2023	7.8	softbus_client_stub in communication subsystem within OpenHarmony-v3.0.5 and prior versions has an authentication bypass	N/A	A-OPE-OPEN-230123/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability which allows an "SA relay attack".Local attackers can bypass authentication and attack other SAs with high privilege. **CVE ID : CVE-2023-0035**		
Authentication Bypass by Capture-replay	09-Jan-2023	7.8	platform_callback_stub in misc subsystem within OpenHarmony-v3.0.5 and prior versions has an authentication bypass vulnerability which allows an "SA relay attack".Local attackers can bypass authentication and attack other SAs with high privilege. **CVE ID : CVE-2023-0036**	N/A	A-OPE-OPEN-230123/123
Vendor: pghero_project					
Product: pghero					
Affected Version(s): From (including) 0.1.1 Up to (excluding) 3.1.0					
Generation of Error Message Containing Sensitive Information	05-Jan-2023	7.5	PgHero before 3.1.0 allows Information Disclosure via EXPLAIN because query results may be present in an error message. (Depending on database user privileges, this may only be information from the database, or may be information from file contents on the database server.) **CVE ID : CVE-2023-22626**	https://github.com/ankane/pghero/issues/439	A-PGH-PGHE-230123/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: protocol					
Product: go-ipld-prime					
Affected Version(s): * Up to (excluding) 0.19.0					
Improper Input Validation	04-Jan-2023	7.5	go-ipld-prime is an implementation of the InterPlanetary Linked Data (IPLD) spec interfaces, a batteries-included codec implementations of IPLD for CBOR and JSON, and tooling for basic operations on IPLD objects. Encoding data which contains a Bytes kind Node will pass a Bytes token to the JSON encoder which will panic as it doesn't expect to receive Bytes tokens. Such an encode should be treated as an error, as plain JSON should not be able to encode Bytes. This only impacts uses of the `json` codec. `dag-json` is not impacted. Use of `json` as a decoder is not impacted. This issue is fixed in v0.19.0. As a workaround, one may prefer the `dag-json` codec, which has the ability to encode bytes. **CVE ID : CVE-2023-22460**	https://github.com/ipld/go-ipld-prime/pull/472	A-PRO-GO-I-230123/125
Vendor: pyload					
Product: pyload					
Affected Version(s): * Up to (excluding) 2023-01-05					
Improper Restriction	05-Jan-2023	6.1	Improper Restriction of Rendered UI Layers or	https://github.com/pylo	A-PYL-PYLO-230123/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Rendered UI Layers or Frames			Frames in GitHub repository pyload/pyload prior to 0.5.0b3.dev33. **CVE ID : CVE-2023-0057**	ad/pyload/commit/bd2a31b7de54570b919aa1581d486e6ee18c0f64, https://hunter.dev/bounties/12b64f91-d048-490c-94b0-37514b6d694d	
Affected Version(s): 0.5.0					
Cleartext Transmission of Sensitive Information	04-Jan-2023	5.3	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository pyload/pyload prior to 0.5.0b3.dev32. **CVE ID : CVE-2023-0055**	https://hunter.dev/bounties/ed88e240-99ff-48a1-bf32-8e1ef5f13cce, https://github.com/pyload/pyload/commit/7b53b8d43c2c072b457dcd19c8a09bcfc3721703	A-PYL-PYLO-230123/127
Vendor: pyload-ng_project					
Product: pyload-ng					
Affected Version(s): * Up to (excluding) 0.5.0b3.dev33					
Improper Restriction of Rendered UI Layers or Frames	05-Jan-2023	6.1	Improper Restriction of Rendered UI Layers or Frames in GitHub repository pyload/pyload prior to 0.5.0b3.dev33. **CVE ID : CVE-2023-0057**	https://github.com/pyload/pyload/commit/bd2a31b7de54570b919aa1581d486e6ee18c0f64, https://hunter.dev/bounti	A-PYL-PYLO-230123/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				es/12b64f91-d048-490c-94b0-37514b6d694d	
Vendor: sanitize-svg_project					
Product: sanitize-svg					
Affected Version(s): * Up to (excluding) 0.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2023	6.1	The `sanitize-svg` package, a small SVG sanitizer to prevent cross-site scripting attacks, uses a deny-list-pattern to sanitize SVGs to prevent XSS. In doing so, literal `<script>`-tags and on-event handlers were detected in versions prior to 0.4.0. As a result, downstream software that relies on `sanitize-svg` and expects resulting SVGs to be safe, may be vulnerable to cross-site scripting. This vulnerability was addressed in v0.4.0. There are no known workarounds **CVE ID : CVE-2023-22461**	https://github.com/mattkrick/sanitize-svg/commit/b107e453ede7b58adccae74a3e474c012eec85d	A-SAN-SANI-230123/129
Vendor: SAP					
Product: bank_account_management					
Affected Version(s): 800					
Exposure of Sensitive Information to an Unauthorized Actor	10-Jan-2023	5.7	In SAP Bank Account Management (Manage Banks) application, when a user clicks a smart link to navigate to another app, personal data is shown directly in the	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e6003	A-SAP-BANK-230123/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URL. They might get captured in log files, bookmarks, and so on disclosing sensitive data of the application. **CVE ID : CVE-2023-0023**	9b.html, https://launchpad.support.sap.com/#/notes/3150704	
Affected Version(s): 900					
Exposure of Sensitive Information to an Unauthorized Actor	10-Jan-2023	5.7	In SAP Bank Account Management (Manage Banks) application, when a user clicks a smart link to navigate to another app, personal data is shown directly in the URL. They might get captured in log files, bookmarks, and so on disclosing sensitive data of the application. **CVE ID : CVE-2023-0023**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3150704	A-SAP-BANK-230123/131
Product: businessobjects_business_intelligence_platform					
Affected Version(s): 420					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	Due to improper input sanitization of user-controlled input in SAP BusinessObjects Business Intelligence Platform CMC application - versions 420, and 430, an attacker with basic user-level privileges can modify/upload crystal reports containing a malicious payload. Once these reports are viewable, anyone who opens those reports would be susceptible to stored XSS attacks. As a result of the attack,	https://launchpad.support.sap.com/#/notes/3266006, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-230123/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information maintained in the victim's web browser can be read, modified, and sent to the attacker. **CVE ID : CVE-2023-0018**		
Affected Version(s): 430					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	Due to improper input sanitization of user-controlled input in SAP BusinessObjects Business Intelligence Platform CMC application - versions 420, and 430, an attacker with basic user-level privileges can modify/upload crystal reports containing a malicious payload. Once these reports are viewable, anyone who opens those reports would be susceptible to stored XSS attacks. As a result of the attack, information maintained in the victim's web browser can be read, modified, and sent to the attacker. **CVE ID : CVE-2023-0018**	https://launchpad.support.sap.com/#/notes/3266006, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-230123/133
Product: business_objects_business_intelligence_platform					
Affected Version(s): 420					
Improper Neutralization of Input During Web Page Generation	10-Jan-2023	5.4	In SAP BusinessObjects Business Intelligence Platform (Web Intelligence user interface) - version 420, some calls return json with wrong content type	https://launchpad.support.sap.com/#/notes/3251447, https://www.sap.com/d	A-SAP-BUSI-230123/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			in the header of the response. As a result, a custom application that calls directly the jsp of Web Intelligence DHTML may be vulnerable to XSS attacks. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-0015**	ocuments/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Product: host_agent					
Affected Version(s): 7.21					
Improper Access Control	10-Jan-2023	6.7	In SAP Host Agent (Windows) - versions 7.21, 7.22, an attacker who gains local membership to SAP_LocalAdmin could be able to replace executables with a malicious file that will be started under a privileged account. Note that by default all user members of SAP_LocaAdmin are denied the ability to logon locally by security policy so that this can only occur if the system has already been compromised. **CVE ID : CVE-2023-0012**	https://launchpad.support.sap.com/#/notes/3276120, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-HOST-230123/135
Affected Version(s): 7.22					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	10-Jan-2023	6.7	In SAP Host Agent (Windows) - versions 7.21, 7.22, an attacker who gains local membership to SAP_LocalAdmin could be able to replace executables with a malicious file that will be started under a privileged account. Note that by default all user members of SAP_LocaAdmin are denied the ability to logon locally by security policy so that this can only occur if the system has already been compromised. **CVE ID : CVE-2023-0012**	https://launchpad.support.sap.com/#/notes/3276120, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-HOST-230123/136
Product: netweaver_application_server_abap					
Affected Version(s): 700					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			illegitimate access to the system. **CVE ID : CVE-2023-0014**		
Affected Version(s): 701					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/138
Affected Version(s): 702					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-0013**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3283283	A-SAP-NETW-230123/140
Affected Version(s): 710					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53,	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-NETW-230123/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	0010-bca6-c68f7e6003 9b.html	
Affected Version(s): 711					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e6003 9b.html	A-SAP-NETW-230123/142
Affected Version(s): 730					
Authentication Bypass by	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702,	https://launchpad.support.sap.com/#/notes/3089	A-SAP-NETW-230123/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 731					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system.	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0014		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-0013**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3283283	A-SAP-NETW-230123/145
Affected Version(s): 740					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			illegitimate access to the system. **CVE ID : CVE-2023-0014**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-0013**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3283283	A-SAP-NETW-230123/147
Affected Version(s): 750					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-0013**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3283283	A-SAP-NETW-230123/149
Affected Version(s): 751					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-0013**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3283283	A-SAP-NETW-230123/151
Affected Version(s): 752					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53,	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-NETW-230123/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	0010-bca6-c68f7e60039b.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-0013**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3283283	A-SAP-NETW-230123/153
Affected Version(s): 753					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/d	A-SAP-NETW-230123/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	ocuments/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-0013**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3283283	A-SAP-NETW-230123/155
Affected Version(s): 754					
Authentication Bypass by	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702,	https://launchpad.support.sap.com/#/notes/3089	A-SAP-NETW-230123/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-0013**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3283283	A-SAP-NETW-230123/157
Affected Version(s): 755					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/158
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3283283	A-SAP-NETW-230123/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0013		
Affected Version(s): 756					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/160
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3283283	A-SAP-NETW-230123/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity of the application. **CVE ID : CVE-2023-0013**		
Affected Version(s): 757					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/162
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jan-2023	6.1	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3283283	A-SAP-NETW-230123/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-0013**		
Product: netweaver_application_server_for_java					
Affected Version(s): 7.50					
Improper Access Control	10-Jan-2023	9.8	An unauthenticated attacker in SAP NetWeaver AS for Java - version 7.50, due to improper access control, can attach to an open interface and make use of an open naming and directory API to access services which can be used to perform unauthorized operations affecting users and data on the current system. This could allow the attacker to have full read access to user data, make modifications to user data, and make services within the system unavailable. **CVE ID : CVE-2023-0017**	https://launchpad.support.sap.com/#/notes/3268093, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/164
Product: netweaver_as_abap_kernel					
Affected Version(s): 7.22					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/d	A-SAP-NETW-230123/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	ocuments/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 7.53					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/166
Affected Version(s): 7.77					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/167
Affected Version(s): 7.81					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			illegitimate access to the system. **CVE ID : CVE-2023-0014**		
Affected Version(s): 7.85					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/169
Affected Version(s): 7.89					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**		
Product: netweaver_as_abap_krnl64nuc					
Affected Version(s): 7.22					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/171
Affected Version(s): 7.22ext					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754,	https://launchpad.support.sap.com/#/notes/3089413, https://ww	A-SAP-NETW-230123/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	w.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Product: netweaver_as_abap_krnl64uc					
Affected Version(s): 7.22					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 7.53					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/174
Affected Version(s): 7.22ext					
Authentication Bypass by Capture-replay	10-Jan-2023	9.8	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by	https://launchpad.support.sap.com/#/notes/3089413, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-230123/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2023-0014**		
Vendor: swifty_page_manager_project					
Product: swifty_page_manager					
Affected Version(s): * Up to (including) 3.0.1					
Cross-Site Request Forgery (CSRF)	05-Jan-2023	8.8	The Swifty Page Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.0.1. This is due to missing or incorrect nonce validation on several AJAX actions handling page creation and deletion among other things. This makes it possible for unauthenticated attackers to invoke those functions, via forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-0088**	N/A	A-SWI-SWIF-230123/176
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2023	4.8	The Swifty Page Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'spm_plugin_options_page_tree_max_width' parameter in versions up to, and including, 3.0.1 due to insufficient input	N/A	A-SWI-SWIF-230123/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-0087**		
Vendor: Synology					
Product: router_manager					
Affected Version(s): From (including) 1.2 Up to (excluding) 1.2.5-8227-6					
Integer Overflow or Wraparound	05-Jan-2023	9.8	Integer overflow or wraparound vulnerability in CGI component in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows remote attackers to overflow buffers via unspecified vectors. **CVE ID : CVE-2023-0077**	https://www.synology.com/en-global/security/advisory/Synology_SA_22_25	A-SYN-ROUT-230123/178
Affected Version(s): From (including) 1.3 Up to (excluding) 1.3.1-9346-3					
Integer Overflow or Wraparound	05-Jan-2023	9.8	Integer overflow or wraparound vulnerability in CGI component in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows remote attackers to	https://www.synology.com/en-global/security/advisory/Synology_SA_22_25	A-SYN-ROUT-230123/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow buffers via unspecified vectors. **CVE ID : CVE-2023-0077**		
Vendor: thinkst					
Product: canarytokens					
Affected Version(s): * Up to (excluding) 2023-01-06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jan-2023	6.1	Canarytokens is an open source tool which helps track activity and actions on your network. A Cross-Site Scripting vulnerability was identified in the history page of triggered Canarytokens prior to sha-fb61290. An attacker who discovers an HTTP-based Canarytoken (a URL) can use this to execute Javascript in the Canarytoken's trigger history page (domain: canarytokens.org) when the history page is later visited by the Canarytoken's creator. This vulnerability could be used to disable or delete the affected Canarytoken, or view its activation history. It might also be used as a stepping stone towards revealing more information about the Canarytoken's creator to the attacker. For example, an attacker could recover the email address tied to the Canarytoken, or place	https://github.com/thinkst/antarytokens/commit/fb612906f2217bbb8863199694891d16e20bad3e, https://github.com/thinkst/canarytokens/security/advisories/GHSA-3h2c-3fgr-74vh	A-THI-CANA-230123/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Javascript on the history page that redirect the creator towards an attacker-controlled Canarytoken to show the creator's network location. This vulnerability is similar to CVE-2022-31113, but affected parameters reported differently from the Canarytoken trigger request. An attacker could only act on the discovered Canarytoken. This issue did not expose other Canarytokens or other Canarytoken creators. Canarytokens Docker images sha-fb61290 and later contain a patch for this issue. **CVE ID : CVE-2023-22475**		
Vendor: tokio					
Product: tokio					
Affected Version(s): From (including) 1.19.0 Up to (excluding) 1.20.3					
Improper Initialization	04-Jan-2023	5.4	Tokio is a runtime for writing applications with Rust. Starting with version 1.7.0 and prior to versions 1.18.4, 1.20.3, and 1.23.1, when configuring a Windows named pipe server, setting `pipe_mode` will reset `reject_remote_clients` to `false`. If the application has previously configured	https://github.com/tokio-rs/tokio/pull/5336	A-TOK-TOKI-230123/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`reject_remote_clients` to `true`, this effectively undoes the configuration. Remote clients may only access the named pipe if the named pipe's associated path is accessible via a publicly shared folder (SMB). Versions 1.23.1, 1.20.3, and 1.18.4 have been patched. The fix will also be present in all releases starting from version 1.24.0. Named pipes were introduced to Tokio in version 1.7.0, so releases older than 1.7.0 are not affected. As a workaround, ensure that `pipe_mode` is set first after initializing a `ServerOptions`. **CVE ID : CVE-2023-22466**		
Affected Version(s): From (including) 1.21.0 Up to (excluding) 1.23.1					
Improper Initialization	04-Jan-2023	5.4	Tokio is a runtime for writing applications with Rust. Starting with version 1.7.0 and prior to versions 1.18.4, 1.20.3, and 1.23.1, when configuring a Windows named pipe server, setting `pipe_mode` will reset `reject_remote_clients` to `false`. If the application has previously configured `reject_remote_clients` to `true`, this effectively undoes the configuration.	https://github.com/tokio-rs/tokio/pull/5336	A-TOK-TOKI-230123/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote clients may only access the named pipe if the named pipe's associated path is accessible via a publicly shared folder (SMB). Versions 1.23.1, 1.20.3, and 1.18.4 have been patched. The fix will also be present in all releases starting from version 1.24.0. Named pipes were introduced to Tokio in version 1.7.0, so releases older than 1.7.0 are not affected. As a workaround, ensure that `pipe_mode` is set first after initializing a `ServerOptions`. **CVE ID : CVE-2023-22466**		
Affected Version(s): From (including) 1.7.0 Up to (excluding) 1.18.4					
Improper Initialization	04-Jan-2023	5.4	Tokio is a runtime for writing applications with Rust. Starting with version 1.7.0 and prior to versions 1.18.4, 1.20.3, and 1.23.1, when configuring a Windows named pipe server, setting `pipe_mode` will reset `reject_remote_clients` to `false`. If the application has previously configured `reject_remote_clients` to `true`, this effectively undoes the configuration. Remote clients may only access the named pipe if the named pipe's	https://github.com/tokio-rs/tokio/pull/5336	A-TOK-TOKI-230123/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			associated path is accessible via a publicly shared folder (SMB). Versions 1.23.1, 1.20.3, and 1.18.4 have been patched. The fix will also be present in all releases starting from version 1.24.0. Named pipes were introduced to Tokio in version 1.7.0, so releases older than 1.7.0 are not affected. As a workaround, ensure that `pipe_mode` is set first after initializing a `ServerOptions`. **CVE ID : CVE-2023-22466**		
Vendor: typelevel					
Product: http4s					
Affected Version(s): 1.0.0					
Improper Input Validation	04-Jan-2023	5.3	Http4s is a Scala interface for HTTP services. Starting with version 0.1.0 and prior to versions 0.21.34, 0.22.15, 0.23.17, and 1.0.0-M38, the `User-Agent` and `Server` header parsers are susceptible to a fatal error on certain inputs. In http4s, modeled headers are lazily parsed, so this only applies to services that explicitly request these typed headers. Fixes are released in 0.21.34, 0.22.15, 0.23.17, and 1.0.0-M38. As a workaround, use the	N/A	A-TYP-HTTP-230123/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			weakly typed header interface. **CVE ID : CVE-2023-22465**		
Affected Version(s): From (including) 0.1.0 Up to (excluding) 0.21.34					
Improper Input Validation	04-Jan-2023	5.3	Http4s is a Scala interface for HTTP services. Starting with version 0.1.0 and prior to versions 0.21.34, 0.22.15, 0.23.17, and 1.0.0-M38, the `User-Agent` and `Server` header parsers are susceptible to a fatal error on certain inputs. In http4s, modeled headers are lazily parsed, so this only applies to services that explicitly request these typed headers. Fixes are released in 0.21.34, 0.22.15, 0.23.17, and 1.0.0-M38. As a workaround, use the weakly typed header interface. **CVE ID : CVE-2023-22465**	N/A	A-TYP-HTTP-230123/185
Affected Version(s): From (including) 0.22.0 Up to (excluding) 0.22.15					
Improper Input Validation	04-Jan-2023	5.3	Http4s is a Scala interface for HTTP services. Starting with version 0.1.0 and prior to versions 0.21.34, 0.22.15, 0.23.17, and 1.0.0-M38, the `User-Agent` and `Server` header parsers are susceptible to a fatal error on certain inputs. In http4s, modeled headers are lazily parsed,	N/A	A-TYP-HTTP-230123/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			so this only applies to services that explicitly request these typed headers. Fixes are released in 0.21.34, 0.22.15, 0.23.17, and 1.0.0-M38. As a workaround, use the weakly typed header interface. **CVE ID : CVE-2023-22465**		
Affected Version(s): From (including) 0.23.0 Up to (excluding) 0.23.17					
Improper Input Validation	04-Jan-2023	5.3	Http4s is a Scala interface for HTTP services. Starting with version 0.1.0 and prior to versions 0.21.34, 0.22.15, 0.23.17, and 1.0.0-M38, the `User-Agent` and `Server` header parsers are susceptible to a fatal error on certain inputs. In http4s, modeled headers are lazily parsed, so this only applies to services that explicitly request these typed headers. Fixes are released in 0.21.34, 0.22.15, 0.23.17, and 1.0.0-M38. As a workaround, use the weakly typed header interface. **CVE ID : CVE-2023-22465**	N/A	A-TYP-HTTP-230123/187
Vendor: usememos					
Product: memos					
Affected Version(s): * Up to (excluding) 0.10.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0. **CVE ID : CVE-2023-0106**	https://huntr.dev/bounties/5c0809cb-f4ff-4447-bed6-b5625fb374bb, https://github.com/usememos/memos/commit/0f8ce3dd1696722f951d7195ad1f88b39a5d15d7	A-USE-MEMO-230123/188
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0. **CVE ID : CVE-2023-0107**	https://huntr.dev/bounties/0b28fa57-acb0-47c8-ac48-962ff3898156, https://github.com/usememos/memos/commit/0f8ce3dd1696722f951d7195ad1f88b39a5d15d7	A-USE-MEMO-230123/189
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0. **CVE ID : CVE-2023-0108**	https://github.com/usememos/memos/commit/46c13a4b7f675b92d297df6dabb4441f13c7cd9c, https://huntr.dev/bounties/f66d33df-6588-4ab4-80a0-	A-USE-MEMO-230123/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				847451517944	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0. **CVE ID : CVE-2023-0110**	https://github.com/usememos/memos/commit/46c13a4b7f675b92d297df6dabb4441f13c7cd9c, https://huntr.dev/bounties/6e4a1961-dbca-46f6-ae21-c25a621e54a7	A-USE-MEMO-230123/191
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0. **CVE ID : CVE-2023-0111**	https://github.com/usememos/memos/commit/46c13a4b7f675b92d297df6dabb4441f13c7cd9c, https://huntr.dev/bounties/70da256c-977a-487e-8a6a-9ae22caedbe3	A-USE-MEMO-230123/192
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0. **CVE ID : CVE-2023-0112**	https://github.com/usememos/memos/commit/46c13a4b7f675b92d297df6dabb4441f13c7cd9c, https://huntr.dev/bounties/ec2a29dc	A-USE-MEMO-230123/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-79a3-44bd-a58b-15f676934af6	
Vendor: Viewvc					
Product: viewvc					
Affected Version(s): * Up to (excluding) 1.1.29					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2023	6.1	ViewVC, a browser interface for CVS and Subversion version control repositories, as a cross-site scripting vulnerability that affects versions prior to 1.2.2 and 1.1.29. The impact of this vulnerability is mitigated by the need for an attacker to have commit privileges to a Subversion repository exposed by an otherwise trusted ViewVC instance. The attack vector involves files with unsafe names (names that, when embedded into an HTML stream, would cause the browser to run unwanted code), which themselves can be challenging to create. Users should update to at least version 1.2.2 (if they are using a 1.2.x version of ViewVC) or 1.1.29 (if they are using a 1.1.x version). ViewVC 1.0.x is no longer supported, so users of that release lineage should implement a workaround. Users can edit their ViewVC EZT	https://github.com/viewvc/viewvc/releases/tag/1.2.2, https://github.com/viewvc/viewvc/releases/tag/1.1.29	A-VIE-VIEW-230123/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			view templates to manually HTML-escape changed paths during rendering. Locate in your template set's `revision.ezt` file references to those changed paths, and wrap them with `[format "html"]` and `[end]`. For most users, that means that references to `[changes.path]` will become `[format "html"][changes.path][end]`. (This workaround should be reverted after upgrading to a patched version of ViewVC, else changed path names will be doubly escaped.) **CVE ID : CVE-2023-22456**		
Affected Version(s): * Up to (excluding) 1.1.30					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2023	5.4	ViewVC is a browser interface for CVS and Subversion version control repositories. Versions prior to 1.2.3 and 1.1.30 are vulnerable to cross-site scripting. The impact of this vulnerability is mitigated by the need for an attacker to have commit privileges to a Subversion repository exposed by an otherwise trusted ViewVC instance. The attack vector involves files with unsafe names (names that, when embedded into an	N/A	A-VIE-VIEW-230123/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTML stream, would cause the browser to run unwanted code), which themselves can be challenging to create. Users should update to at least version 1.2.3 (if they are using a 1.2.x version of ViewVC) or 1.1.30 (if they are using a 1.1.x version). ViewVC 1.0.x is no longer supported, so users of that release lineage should implement one of the following workarounds. Users can edit their ViewVC EZT view templates to manually HTML-escape changed path "copyfrom paths" during rendering. Locate in your template set's `revision.ezt` file references to those changed paths, and wrap them with `[format "html"]` and `[end]`. For most users, that means that references to `[changes.copy_path]` will become `[format "html"][changes.copy_path][end]`. (This workaround should be reverted after upgrading to a patched version of ViewVC, else "copyfrom path" names will be doubly escaped.) **CVE ID : CVE-2023-22464**		
Affected Version(s): From (including) 1.2.0 Up to (excluding) 1.2.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2023	6.1	ViewVC, a browser interface for CVS and Subversion version control repositories, as a cross-site scripting vulnerability that affects versions prior to 1.2.2 and 1.1.29. The impact of this vulnerability is mitigated by the need for an attacker to have commit privileges to a Subversion repository exposed by an otherwise trusted ViewVC instance. The attack vector involves files with unsafe names (names that, when embedded into an HTML stream, would cause the browser to run unwanted code), which themselves can be challenging to create. Users should update to at least version 1.2.2 (if they are using a 1.2.x version of ViewVC) or 1.1.29 (if they are using a 1.1.x version). ViewVC 1.0.x is no longer supported, so users of that release lineage should implement a workaround. Users can edit their ViewVC EZT view templates to manually HTML-escape changed paths during rendering. Locate in your template set's `revision.ezt` file references to those changed paths, and wrap	https://github.com/viewvc/viewvc/releases/tag/1.2.2, https://github.com/viewvc/viewvc/releases/tag/1.1.29	A-VIE-VIEW-230123/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			them with `[format "html"]` and `[end]`. For most users, that means that references to `[changes.path]` will become `[format "html"][changes.path][end]`. (This workaround should be reverted after upgrading to a patched version of ViewVC, else changed path names will be doubly escaped.) **CVE ID : CVE-2023-22456**		
Affected Version(s): From (including) 1.2.0 Up to (excluding) 1.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2023	5.4	ViewVC is a browser interface for CVS and Subversion version control repositories. Versions prior to 1.2.3 and 1.1.30 are vulnerable to cross-site scripting. The impact of this vulnerability is mitigated by the need for an attacker to have commit privileges to a Subversion repository exposed by an otherwise trusted ViewVC instance. The attack vector involves files with unsafe names (names that, when embedded into an HTML stream, would cause the browser to run unwanted code), which themselves can be challenging to create. Users should update to at least version 1.2.3 (if they are using a 1.2.x	N/A	A-VIE-VIEW-230123/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version of ViewVC) or 1.1.30 (if they are using a 1.1.x version). ViewVC 1.0.x is no longer supported, so users of that release lineage should implement one of the following workarounds. Users can edit their ViewVC EZT view templates to manually HTML-escape changed path "copyfrom paths" during rendering. Locate in your template set's `revision.ezt` file references to those changed paths, and wrap them with `[format "html"]` and `[end]`. For most users, that means that references to `[changes.copy_path]` will become `[format "html"][changes.copy_path][end]`. (This workaround should be reverted after upgrading to a patched version of ViewVC, else "copyfrom path" names will be doubly escaped.) **CVE ID : CVE-2023-22464**		
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 9.0.1143					
Out-of-bounds Read	04-Jan-2023	7.8	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.1143.	https://github.com/vim/vim/commit/7b17eb4b063a234376	A-VIM-VIM-230123/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0049	c1ec909ee293e42cff290c, https://huntr.dev/bounties/5e6f325c-ba54-4bf0-b050-dca048fd3fd9	
Affected Version(s): * Up to (excluding) 9.0.1144					
Heap-based Buffer Overflow	04-Jan-2023	7.8	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1144. **CVE ID : CVE-2023-0051**	https://huntr.dev/bounties/1c8686db-baa6-42dc-ba45-aed322802de9, https://github.com/vim/vim/commit/c32949b0779106ed5710ae3bffc5053e49083ab4	A-VIM-VIM-230123/199
Affected Version(s): * Up to (excluding) 9.0.1145					
Out-of-bounds Write	04-Jan-2023	7.8	Out-of-bounds Write in GitHub repository vim/vim prior to 9.0.1145. **CVE ID : CVE-2023-0054**	https://huntr.dev/bounties/b289ee0f-fd16-4147-bd01-c6289c45e49d, https://github.com/vim/vim/commit/3ac1d97a1d9353490493d30088256360435f7731	A-VIM-VIM-230123/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Wordpress					
Product: wordpress					
Affected Version(s): * Up to (including) 6.1.1					
Uncontrolled Resource Consumption	05-Jan-2023	7.5	WordPress through 6.1.1 depends on unpredictable client visits to cause wp-cron.php execution and the resulting security updates, and the source code describes "the scenario where a site may not receive enough visits to execute scheduled tasks in a timely manner," but neither the installation guide nor the security guide mentions this default behavior, or alerts the user about security risks on installations with very few visits. **CVE ID : CVE-2023-22622**	https://developer.wordpress.org/plugins/cron/, https://wordpress.org/about/security/, https://wordpress.org/support/article/how-to-install-wordpress/	A-WOR-WORD-230123/201
Vendor: Xwiki					
Product: ckeditor_integration					
Affected Version(s): * Up to (excluding) 1.64.3					
Cross-Site Request Forgery (CSRF)	04-Jan-2023	8.8	CKEditor Integration UI adds support for editing wiki pages using CKEditor. Prior to versions 1.64.3,t he `CKEditor.HTMLConverter` document lacked a protection against Cross-Site Request Forgery (CSRF), allowing to execute macros with the rights of the current user.	https://jira.xwiki.org/browse/CKEDITOR-475, https://github.com/xwiki-contrib/application-ckeditor/commit/6b1053164386aefc	A-XWI-CKED-230123/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If a privileged user with programming rights was tricked into executing a GET request to this document with certain parameters (e.g., via an image with a corresponding URL embedded in a comment or via a redirect), this would allow arbitrary remote code execution and the attacker could gain rights, access private information or impact the availability of the wiki. The issue has been patched in the CKEditor Integration version 1.64.3. This has also been patched in the version of the CKEditor integration that is bundled starting with XWiki 14.6 RC1. There are no known workarounds for this other than upgrading the CKEditor integration to a fixed version. **CVE ID : CVE-2023-22457**	526df7512bc664918aa6849b, https://github.com/xwiki-contrib/application-ckeditor/security/advisories/GHSA-6mjp-2rm6-9g85	
Vendor: zip4j_project					
Product: zip4j					
Affected Version(s): * Up to (including) 2.11.2					
Origin Validation Error	10-Jan-2023	5.9	Zip4j through 2.11.2, as used in Threema and other products, does not always check the MAC when decrypting a ZIP archive.	https://threema.ch/en/blog/posts/news-alleged-weaknesses-statement	A-ZIP-ZIP4-230123/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22899		
Hardware					
Vendor: multilaserempresas					
Product: re708					
Affected Version(s): -					
N/A	01-Jan-2023	7.5	A vulnerability was found in Multilaser RE708 RE1200R4GC-2T2R-V3_v3411b_MUL029B. It has been rated as problematic. This issue affects some unknown processing of the component Telnet Service. The manipulation leads to denial of service. The attack may be initiated remotely. The identifier VDB-217169 was assigned to this vulnerability. **CVE ID : CVE-2023-0029**	N/A	H-MUL-RE70-230123/204
Vendor: netis-systems					
Product: netcore_router					
Affected Version(s): -					
Exposure of Sensitive Information to an Unauthorized Actor	07-Jan-2023	7.5	A vulnerability was found in Netis Netcore Router. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file param.file.tgz of the component Backup Handler. The manipulation leads to	N/A	H-NET-NETC-230123/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-217591. **CVE ID : CVE-2023-0113**		
Cleartext Storage in a File or on Disk	07-Jan-2023	5.5	A vulnerability was found in Netis Netcore Router. It has been rated as problematic. Affected by this issue is some unknown functionality of the file param.file.tgz of the component Backup Handler. The manipulation leads to cleartext storage in a file or on disk. Local access is required to approach this attack. The identifier of this vulnerability is VDB-217592. **CVE ID : CVE-2023-0114**	N/A	H-NET-NETC-230123/206
Operating System					
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 36					
Out-of-bounds Read	04-Jan-2023	7.8	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.1143. **CVE ID : CVE-2023-0049**	https://github.com/vim/vim/commit/7b17eb4b063a234376c1ec909ee293e42cff290c, https://huntr.dev/bounties/5e6f325c	O-FED-FEDO-230123/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-ba54-4bf0-b050-dca048fd3fd9	
Affected Version(s): 37					
Out-of-bounds Read	04-Jan-2023	7.8	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.1143. **CVE ID : CVE-2023-0049**	https://github.com/vim/vim/commit/7b17eb4b063a234376c1ec909ee293e42cff290c, https://hunter.dev/bounties/5e6f325c-ba54-4bf0-b050-dca048fd3fd9	O-FED-FEDO-230123/208
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	10-Jan-2023	8.8	Inappropriate implementation in in Fullscreen API in Google Chrome on Android prior to 109.0.5414.74 allowed a remote attacker to execute incorrect security UI via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-0136**	https://crbug.com/1356987, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	O-GOO-ANDR-230123/209
N/A	10-Jan-2023	6.5	Inappropriate implementation in in Permission prompts in Google Chrome on Android prior to	https://crbug.com/1375132, https://chromereleases.g	O-GOO-ANDR-230123/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			109.0.5414.74 allowed a remote attacker to bypass main origin permission delegation via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-0133**	oogleblog.com/2023/01/stable-channel-update-for-desktop.html	
Product: chrome_os					
Affected Version(s): -					
Use After Free	10-Jan-2023	8.8	Use after free in Overview Mode in Google Chrome on Chrome OS prior to 109.0.5414.74 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0128**	https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	O-GOO-CHRO-230123/211
Out-of-bounds Write	10-Jan-2023	8.8	Heap buffer overflow in Platform Apps in Google Chrome on Chrome OS prior to 109.0.5414.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-0137**	https://crbug.com/1399904, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	O-GOO-CHRO-230123/212
Vendor: Microsoft					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows					
Affected Version(s): -					
Improper Access Control	10-Jan-2023	6.7	In SAP Host Agent (Windows) - versions 7.21, 7.22, an attacker who gains local membership to SAP_LocalAdmin could be able to replace executables with a malicious file that will be started under a privileged account. Note that by default all user members of SAP_LocaAdmin are denied the ability to logon locally by security policy so that this can only occur if the system has already been compromised. **CVE ID : CVE-2023-0012**	https://launchpad.support.sap.com/#/notes/3276120, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	O-MIC-WIND-230123/213
N/A	10-Jan-2023	6.5	Inappropriate implementation in in Permission prompts in Google Chrome on Windows prior to 109.0.5414.74 allowed a remote attacker to force acceptance of a permission prompt via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-0132**	https://crbug.com/1371215, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	O-MIC-WIND-230123/214
Improper Input Validation	10-Jan-2023	6.5	Insufficient validation of untrusted input in Downloads in Google Chrome on Windows	https://chromereleases.googleblog.com/2023/01	O-MIC-WIND-230123/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 109.0.5414.74 allowed a remote attacker to bypass download restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-0139**	/stable-channel-update-for-desktop.html, https://crbug.com/1367632	
N/A	10-Jan-2023	6.5	Inappropriate implementation in in File System API in Google Chrome on Windows prior to 109.0.5414.74 allowed a remote attacker to bypass file system restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-0140**	https://crbug.com/1326788, https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop.html	O-MIC-WIND-230123/216
Vendor: multilaserempresas					
Product: re708_firmware					
Affected Version(s): re1200r4gc-2t2r-v3_v3411b_mul029b					
N/A	01-Jan-2023	7.5	A vulnerability was found in Multilaser RE708 RE1200R4GC-2T2R-V3_v3411b_MUL029B. It has been rated as problematic. This issue affects some unknown processing of the component Telnet Service. The manipulation leads to denial of service. The attack may be initiated remotely. The identifier VDB-217169 was	N/A	O-MUL-RE70-230123/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-0029**		
Vendor: netis-systems					
Product: netcore_router_firmware					
Affected Version(s): -					
Exposure of Sensitive Information to an Unauthorized Actor	07-Jan-2023	7.5	A vulnerability was found in Netis Netcore Router. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file param.file.tgz of the component Backup Handler. The manipulation leads to information disclosure. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-217591. **CVE ID : CVE-2023-0113**	N/A	O-NET-NETC-230123/218
Cleartext Storage in a File or on Disk	07-Jan-2023	5.5	A vulnerability was found in Netis Netcore Router. It has been rated as problematic. Affected by this issue is some unknown functionality of the file param.file.tgz of the component Backup Handler. The manipulation leads to cleartext storage in a file or on disk. Local access is required to approach this attack. The identifier of	N/A	O-NET-NETC-230123/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability is VDB-217592. **CVE ID : CVE-2023-0114**		