National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 – 15 Jun 2024 Vol. 11 No. 11
https://nciipc.gov.in/

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 10web					
Product: photo_gallery					
Affected Version(s): * Up to (excluding) 1.8.24					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jun-2024	8.8	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.8.23 via the esc_dir function. This makes it possible for authenticated attackers to cut and paste (copy) the contents of arbitrary files on the server, which can contain sensitive information, and to cut (delete) arbitrary directories, including the root WordPress directory. By default this can be exploited by administrators only. In the premium version of the plugin, administrators can give gallery edit permissions to lower level users,	https://plugins.trac.wordpress.org/changeset/3098798/	A-10W-PHOT-200624/1

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which might make this exploitable by users as low as contributors. **CVE ID: CVE-2024-5481**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	5.4	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'svg' parameter in all versions up to, and including, 1.8.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, this can only be exploited by administrators, but the ability to use and configure Photo Gallery can be extended to contributors on pro versions of the plugin. **CVE ID: CVE-2024-5426**	https://plugins.trac.wordpress.org/changeset/3098798/	A-10W-PHOT-200624/2

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: 83pixel					
Product: simple_cod_fees_for_woocommerce					
Affected Version(s): * Up to (including) 2.0.2					
Missing Authorization	09-Jun-2024	8.8	Missing Authorization vulnerability in Andreas Sofantzis Simple COD Fees for WooCommerce.This issue affects Simple COD Fees for WooCommerce: from n/a through 2.0.2. **CVE ID: CVE-2024-35662**	N/A	A-83P-SIMP-200624/3
Vendor: actpro					
Product: extra_product_options_for_woocommerce					
Affected Version(s): * Up to (excluding) 3.0.7					
Missing Authorization	10-Jun-2024	8.8	Missing Authorization vulnerability in actpro Extra Product Options for WooCommerce.This issue affects Extra Product Options for WooCommerce: from n/a through 3.0.6. **CVE ID: CVE-2024-35727**	N/A	A-ACT-EXTR-200624/4
Vendor: acurax					
Product: under_construction_\/_maintenance_mode					
Affected Version(s): * Up to (including) 2.6					
Authentication Bypass	10-Jun-2024	5.3	Authentication Bypass by Spoofing vulnerability in	N/A	A-ACU-UNDE-200624/5

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
by Spoofing			Acurax Under Construction / Maintenance Mode from Acurax allows Authentication Bypass.This issue affects Under Construction / Maintenance Mode from Acurax: from n/a through 2.6. **CVE ID: CVE-2024-35749**		
Vendor: Adobe					
Product: experience_manager					
Affected Version(s): * Up to (excluding) 2024.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	6.1	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-36216**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/6
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS)	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-20769**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-20784**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/8
Improper Neutralization of Input During Web Page	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26036**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. **CVE ID: CVE-2024-26037**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/10

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-26039**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/11
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-26053**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26054**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/13
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/14

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script. **CVE ID: CVE-2024-26055**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the malicious script. **CVE ID: CVE-2024-26057**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/15

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. **CVE ID: CVE-2024-26058**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/16
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/17

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. **CVE ID: CVE-2024-26060**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26066**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/18
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/19

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID: CVE-2024-26068**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26070**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/20
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/21

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26071**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute. **CVE ID: CVE-2024-26072**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/22
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/23

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26074**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26075**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/24
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/25

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26077**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26078**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/26
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/27

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26081**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26082**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/28
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/29

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26083**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26085**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/30
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS)	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/31

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26086**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26088**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/32
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS)	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/33

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script. **CVE ID: CVE-2024-26089**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. **CVE ID: CVE-2024-26090**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/34

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute. **CVE ID: CVE-2024-26091**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/35
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26092**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26093**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/37
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/38

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26095**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26110**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/39
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within the context of the victim's browser. **CVE ID: CVE-2024-26111**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26113**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/41
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the victim's browser. **CVE ID: CVE-2024-26114**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26115**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/43
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/44

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-26116		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26117**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/45
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/46

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-26121		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26123**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/47
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/48

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. **CVE ID: CVE-2024-34119**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-34120**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/49
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/50

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36141**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36142**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/51
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36143**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36144**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/53
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/54

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36147**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/55
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/56

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36148**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36149**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/57
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/58

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script. **CVE ID: CVE-2024-36151**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/59
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/60

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36152**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36153**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/61
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/62

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36154**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36155**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/63
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/64

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36156**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36157**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/65
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS)	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/66

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36158**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36159**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/67
Improper Neutralization of Input During Web Page	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36160**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36161**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/69
Improper Neutralization of Input During	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36162**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36163**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/71
Improper Neutralization of Input	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier	https://helpx.adobe.com/security/products/ex	A-ADO-EXPE-200624/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36164**	perience-manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36165**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/73

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36166**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/74
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/75

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36167		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36168**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/76
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. **CVE ID: CVE-2024-36169**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36170**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/78
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID: CVE-2024-36171**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36172**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/80
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/81

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36173**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36174**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/82
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36175**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36176**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/84
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/85

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36178**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/86
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/87

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36179**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36180**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/88
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/89

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser session. Exploitation of this issue requires user interaction, typically in the form of convincing a victim to visit a maliciously crafted web page or to interact with a maliciously modified DOM element within the application. **CVE ID: CVE-2024-36181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36182**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/90
Improper Neutralization of Input During	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. **CVE ID: CVE-2024-36183**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a malicious link or to submit a	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/92

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted form. **CVE ID: CVE-2024-36184**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36185**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/93
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID: CVE-2024-36186**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36187**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/95
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/96

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36188**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36189**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/97
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-36190**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36191**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/99
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/100

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36192**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36193**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/101
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/102

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36194**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36195**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/103
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/104

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36196**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-36197**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/105
Improper Neutralization of Input	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier	https://helpx.adobe.com/security/products/ex	A-ADO-EXPE-200624/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36198**	perience-manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36199**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/107

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36200**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/108
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/109

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36201		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36202**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/110
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. **CVE ID: CVE-2024-36203**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36204**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/112
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID: CVE-2024-36205**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-36206**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/114
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/115

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. **CVE ID: CVE-2024-36207**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36208**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/116
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID: CVE-2024-36209**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-36210**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/118
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the victim's browser. **CVE ID: CVE-2024-36211**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36212**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/120
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID: CVE-2024-36213**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36214**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/122
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36215**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36217**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/124
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36218**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36219**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/126
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/127

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script. **CVE ID: CVE-2024-36220**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36221**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/128
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-36222**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable script to execute. **CVE ID: CVE-2024-36224**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36225**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/131
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/132

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. **CVE ID: CVE-2024-36227**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-36228**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/133
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. **CVE ID: CVE-2024-36229**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/135

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36230		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script. **CVE ID: CVE-2024-36231**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/136
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/137

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36232**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a malicious link. **CVE ID: CVE-2024-36233**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/138
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/139

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-36234**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script. **CVE ID: CVE-2024-36235**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/140

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. **CVE ID: CVE-2024-36236**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/141
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			click on a malicious link or to interact with a maliciously crafted web page. **CVE ID: CVE-2024-36238**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. **CVE ID: CVE-2024-36239**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/143
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	4.8	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a privileged attacker to inject malicious scripts into vulnerable form fields.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/144

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26049**		
Affected Version(s): * Up to (excluding) 6.5.21					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	6.1	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-36216**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/145
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-20769**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-20784**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/147
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/148

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26036**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. **CVE ID: CVE-2024-26037**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/149
Improper Neutralization of Input During Web Page	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-26039**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/151

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form that triggers the vulnerability. **CVE ID: CVE-2024-26053**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26054**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/152
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/153

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script. **CVE ID: CVE-2024-26055**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the malicious script. **CVE ID: CVE-2024-26057**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/154
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. **CVE ID: CVE-2024-26058**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26060**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/156
Improper Neutralization of Input	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier	https://helpx.adobe.com/security/products/ex	A-ADO-EXPE-200624/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26066**	perience-manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26068**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/158

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26070**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/159
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/160

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-26071		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute. **CVE ID: CVE-2024-26072**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/161
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26074**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26075**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/163
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/164

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26077**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26078**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/165
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/166

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26081**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26082**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/167
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26083**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26085**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/169
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/170

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26086**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26088**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/171
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/172

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script. **CVE ID: CVE-2024-26089**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. **CVE ID: CVE-2024-26090**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/173
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute. **CVE ID: CVE-2024-26091**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/175

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-26092		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26093**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/176
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/177

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-26095		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26110**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/178
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/179

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-26111		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26113**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/180
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26114**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/181

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26115**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/182
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26116**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/183
Improper Neutralization of Input	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier	https://helpx.adobe.com/security/products/ex	A-ADO-EXPE-200624/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-26117**	perience-manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26121**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/185
Improper Neutralization of Input During	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/186

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26123**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-34119**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/187
Improper Neutralization of Input	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier	https://helpx.adobe.com/security/products/ex	A-ADO-EXPE-200624/188

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-34120**	perience-manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36141**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/189

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36142**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/190
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/191

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36143		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36144**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/192
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. **CVE ID: CVE-2024-36146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36147**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/194
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/195

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID: CVE-2024-36148**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36149**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/196
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/197

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script. **CVE ID: CVE-2024-36151**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/198
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/199

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36152**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36153**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/200
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/201

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36154**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36155**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/202
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/203

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36156**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36157**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/204
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/205

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36158**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36159**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/206
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/207

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36160**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36161**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/208
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/209

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36162**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36163**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/210
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/211

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36164**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36165**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/212
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS)	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36166**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36167**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/214
Improper Neutralization of Input During Web Page	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36168**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36169**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/216
Improper Neutralization of Input During	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36170**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36171**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/218
Improper Neutralization of Input	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier	https://helpx.adobe.com/security/products/ex	A-ADO-EXPE-200624/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36172**	perience-manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36173**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/220

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36174**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/221
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/222

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36175		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36176**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/223
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. **CVE ID: CVE-2024-36177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36178**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/225
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/226

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID: CVE-2024-36179**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36180**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/227
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/228

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction, typically in the form of convincing a victim to visit a maliciously crafted web page or to interact with a maliciously modified DOM element within the application. **CVE ID: CVE-2024-36181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36182**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/229
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/230

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. **CVE ID: CVE-2024-36183**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a malicious link or to submit a specially crafted form. **CVE ID: CVE-2024-36184**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/231

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36185**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/232
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/233

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36186		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36187**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/234
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. **CVE ID: CVE-2024-36188**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36189**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/236
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/237

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-36190**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36191**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/238
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36192**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36193**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/240
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36194**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36195**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/242
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/243

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36196**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-36197**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/244
Improper Neutralization of Input During Web Page	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36198**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36199**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/246
Improper Neutralization of Input During	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-200624/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36200**	manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36201**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/248
Improper Neutralization of Input	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier	https://helpx.adobe.com/security/products/ex	A-ADO-EXPE-200624/249

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36202**	perience-manager/apsb24-28.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36203**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/250

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36204**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/251
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/252

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36205		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-36206**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/253
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/254

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36207		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36208**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/255
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/256

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. **CVE ID: CVE-2024-36209**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-36210**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/257
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the victim's browser. **CVE ID: CVE-2024-36211**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36212**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/259
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/260

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID: CVE-2024-36213**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36214**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/261
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/262

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36215**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36217**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/263
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36218**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36219**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/265
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/266

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script. **CVE ID: CVE-2024-36220**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36221**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/267
Improper Neutralization of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/268

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-36222**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/269

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable script to execute. **CVE ID: CVE-2024-36224**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36225**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/270
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/271

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. **CVE ID: CVE-2024-36227**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-36228**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/272
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. **CVE ID: CVE-2024-36229**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/274

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36230		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script. **CVE ID: CVE-2024-36231**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/275
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/276

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-36232**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a malicious link. **CVE ID: CVE-2024-36233**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/277
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/278

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability. **CVE ID: CVE-2024-36234**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script. **CVE ID: CVE-2024-36235**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/279

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. **CVE ID: CVE-2024-36236**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/280
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			click on a malicious link or to interact with a maliciously crafted web page. **CVE ID: CVE-2024-36238**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. **CVE ID: CVE-2024-36239**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/282
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	4.8	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a privileged attacker to inject malicious scripts into vulnerable form fields.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-200624/283

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-26049**		
Vendor: apport_project					
Product: apport					
Affected Version(s): * Up to (excluding) 2.21.0					
N/A	04-Jun-2024	7.8	Apport does not disable python crash handler before entering chroot **CVE ID: CVE-2022-28657**	N/A	A-APP-APPO-200624/284
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.1	is_closing_session() allows users to create arbitrary tcp dbus connections **CVE ID: CVE-2022-28655**	N/A	A-APP-APPO-200624/285
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	04-Jun-2024	5.5	~/.config/apport/settings parsing is vulnerable to "billion laughs" attack **CVE ID: CVE-2022-28652**	N/A	A-APP-APPO-200624/286
Allocation of Resources	04-Jun-2024	5.5	is_closing_session() allows users to fill up apport.log	N/A	A-APP-APPO-200624/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			**CVE ID: CVE-2022-28654**		
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to consume RAM in the Apport process **CVE ID: CVE-2022-28656**	N/A	A-APP-APPO-200624/288
N/A	04-Jun-2024	5.5	Apport argument parsing mishandles filename splitting on older kernels resulting in argument spoofing **CVE ID: CVE-2022-28658**	N/A	A-APP-APPO-200624/289
Vendor: ARM					
Product: bifrost_gpu_kernel_driver					
Affected Version(s): From (including) r34p0 Up to (excluding) r41p0					
Use After Free	07-Jun-2024	5.5	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver allows a local non-privileged user to make improper GPU memory processing operations to gain access to already freed memory.This issue affects Bifrost GPU Kernel Driver: from r34p0 through r40p0; Valhall GPU Kernel Driver: from r34p0 through r40p0.	https://developer.arm.com/Arm Security Center/Mali GPU Driver Vulnerabilities	A-ARM-BIFR-200624/290

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-4610		
Product: valhall_gpu_kernel_driver					
Affected Version(s): From (including) r34p0 Up to (excluding) r41p0					
Use After Free	07-Jun-2024	5.5	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver allows a local non-privileged user to make improper GPU memory processing operations to gain access to already freed memory.This issue affects Bifrost GPU Kernel Driver: from r34p0 through r40p0; Valhall GPU Kernel Driver: from r34p0 through r40p0. **CVE ID: CVE-2024-4610**	https://developer.arm.com/Arm Security Center/Mali GPU Driver Vulnerabilities	A-ARM-VALH-200624/291
Vendor: arwebdesign					
Product: dashboard_to-do_list					
Affected Version(s): * Up to (excluding) 1.3.0					
Missing Authorization	10-Jun-2024	8.8	Missing Authorization vulnerability in Andrew Rapps Dashboard To-Do List.This issue affects Dashboard To-Do List: from n/a through 1.2.0.	N/A	A-ARW-DASH-200624/292

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-35723		
Vendor: authlib					
Product: authlib					
Affected Version(s): * Up to (excluding) 1.3.1					
Improper Verification of Cryptographic Signature	09-Jun-2024	7.5	lepture Authlib before 1.3.1 has algorithm confusion with asymmetric public keys. Unless an algorithm is specified in a jwt.decode call, HMAC verification is allowed with any asymmetric public key. (This is similar to CVE-2022-29217 and CVE-2024-33663.) **CVE ID: CVE-2024-37568**	N/A	A-AUT-AUTH-200624/293
Vendor: autowriter					
Product: ai_post_generator_|_autowriter					
Affected Version(s): * Up to (excluding) 3.4					
Missing Authorization	09-Jun-2024	8.8	Missing Authorization vulnerability in AutoWriter AI Post Generator | AutoWriter.This issue affects AI Post Generator | AutoWriter: from n/a through 3.3. **CVE ID: CVE-2024-32713**	N/A	A-AUT-AI_P-200624/294
Vendor: Avast					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: antivirus					
Affected Version(s): * Up to (excluding) 24.2					
Improper Link Resolution Before File Access ('Link Following')	10-Jun-2024	7	A sym-linked file accessed via the repair function in Avast Antivirus <24.2 on Windows may allow user to elevate privilege to delete arbitrary files or run processes as NT AUTHORITY\SYSTEM. The vulnerability exists within the "Repair" (settings -> troubleshooting -> repair) feature, which attempts to delete a file in the current user's AppData directory as NT AUTHORITY\SYSTEM. A low-privileged user can make a pseudo-symlink and a junction folder and point to a file on the system. This can provide a low-privileged user an Elevation of Privilege to win a race-condition which will re-create the system files and make Windows callback to a specially-crafted file which	N/A	A-AVA-ANTI-200624/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could be used to launch a privileged shell instance. This issue affects Avast Antivirus prior to 24.2. **CVE ID: CVE-2024-5102**		
Vendor: awplife					
Product: image_gallery					
Affected Version(s): * Up to (excluding) 1.4.6					
Missing Authorization	10-Jun-2024	8.8	Missing Authorization vulnerability in AWP Life Image Gallery – Lightbox Gallery, Responsive Photo Gallery, Masonry Gallery.This issue affects Image Gallery – Lightbox Gallery, Responsive Photo Gallery, Masonry Gallery: from n/a through 1.4.5. **CVE ID: CVE-2024-35721**	N/A	A-AWP-IMAG-200624/296
Product: slider_responsive_slideshow					
Affected Version(s): * Up to (excluding) 1.4.2					
Missing Authorization	10-Jun-2024	8.8	Missing Authorization vulnerability in AWP Life Slider Responsive Slideshow – Image slider, Gallery slideshow.This	N/A	A-AWP-SLID-200624/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects Slider Responsive Slideshow – Image slider, Gallery slideshow: from n/a through 1.4.0. **CVE ID: CVE-2024-35722**		
Vendor: bakery_online_ordering_system_project					
Product: bakery_online_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jun-2024	9.8	A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument txtsearch leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-267091. **CVE ID: CVE-2024-5635**	N/A	A-BAK-BAKE-200624/298
Improper Neutralization of	05-Jun-2024	9.8	A vulnerability was found in itsourcecode	N/A	A-BAK-BAKE-200624/299

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Bakery Online Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file report/index.php. The manipulation of the argument procduct leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-267092. **CVE ID: CVE-2024-5636**		
Vendor: beyondtrust					
Product: beyondinsight					
Affected Version(s): * Up to (excluding) 23.1					
N/A	04-Jun-2024	5.3	Prior to 23.1, an information disclosure vulnerability exists within BeyondInsight which can allow an attacker to enumerate usernames. **CVE ID: CVE-2024-4220**	https://www.beyondtrust.com/trust-center/security-advisories/BT24-06	A-BEY-BEYO-200624/300
Affected Version(s): * Up to (excluding) 23.2					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	04-Jun-2024	9.1	Prior to 23.2, it is possible to perform arbitrary Server-Side requests via HTTP-based connectors within BeyondInsight, resulting in a server-side request forgery vulnerability. **CVE ID: CVE-2024-4219**	https://www.beyondtrust.com/trust-center/security-advisories/BT24-05	A-BEY-BEYO-200624/301
Vendor: Bitdefender					
Product: gravityzone					
Affected Version(s): * Up to (excluding) 6.38.1-2					
Server-Side Request Forgery (SSRF)	06-Jun-2024	9.8	A host whitelist parser issue in the proxy service implemented in the GravityZone Update Server allows an attacker to cause a server-side request forgery. This issue only affects GravityZone Console versions before 6.38.1-2 that are running only on premise. **CVE ID: CVE-2024-4177**	N/A	A-BIT-GRAV-200624/302
Vendor: born05					
Product: two-factor_authentication					
Affected Version(s): * Up to (excluding) 3.3.4					
Improper Authentication	06-Jun-2024	6.5	The CraftCMS plugin Two-Factor Authentication	N/A	A-BOR-TWO--200624/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 3.3.3 allows reuse of TOTP tokens multiple times within the validity period. **CVE ID: CVE-2024-5658**		
Affected Version(s): From (including) 3.3.1 Up to (excluding) 3.3.4					
Insufficiently Protected Credentials	06-Jun-2024	8.1	The CraftCMS plugin Two-Factor Authentication in versions 3.3.1, 3.3.2 and 3.3.3 discloses the password hash of the currently authenticated user after submitting a valid TOTP. **CVE ID: CVE-2024-5657**	N/A	A-BOR-TWO--200624/304
Vendor: bosathemes					
Product: bosa_elementor_addons_and_templates_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.0.13					
Missing Authorization	10-Jun-2024	8.8	Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce.This issue affects Bosa Elementor Addons and Templates for WooCommerce: from n/a through 1.0.12. **CVE ID: CVE-2024-35724**	N/A	A-BOS-BOSA-200624/305
Vendor: brizy					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: brizy-page_builder					
Affected Version(s): * Up to (excluding) 2.4.42					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post content in all versions up to, and including, 2.4.41 due to insufficient input sanitization performed only on the client side and insufficient output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-1940**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3055256%40brizy&new=3055256%40brizy&sfp_email=&sfph_mail=	A-BRI-BRIZ-200624/306
Affected Version(s): * Up to (excluding) 2.4.44					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	6.1	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form name values in all versions up to, and including, 2.4.43 due to insufficient input	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3086506%40brizy%2Ftrunk&old=3058896%40brizy%2Ftrunk&s	A-BRI-BRIZ-200624/307

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-2087**	fp_email=&sfph_mail=	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Custom Attributes for blocks in all versions up to, and including, 2.4.43 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-1161**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3086506%40brizy%2Ftrunk&old=3058896%40brizy%2Ftrunk&sfp_email=&sfph_mail=	A-BRI-BRIZ-200624/308

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Link To' field of multiple widgets in all versions up to, and including, 2.4.43 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-3667**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3086506%40brizy%2Ftrunk&old=3058896%40brizy%2Ftrunk&sfp_email=&sfph_mail=	A-BRI-BRIZ-200624/309
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's contact form widget error message and redirect URL in all versions up to, and including, 2.4.43 due to insufficient input sanitization	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3086506%40brizy%2Ftrunk&old=3058896%40brizy%2Ftrunk&sfp_email=&sfph_mail=	A-BRI-BRIZ-200624/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and output escaping on user supplied error messages. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-1164**		
Vendor: buddyboss					
Product: buddyboss_platform					
Affected Version(s): * Up to (excluding) 2.6.00					
Authorization Bypass Through User-Controlled Key	05-Jun-2024	4.3	The contains an IDOR vulnerability that allows a user to comment on a private post by manipulating the ID included in the request **CVE ID: CVE-2024-4886**	N/A	A-BUD-BUDD-200624/311
Vendor: buddypress_cover_project					
Product: buddypress_cover					
Affected Version(s): * Up to (including) 2.1.4.2					
Unrestricted Upload of File with Dangerous Type	10-Jun-2024	9.8	Unrestricted Upload of File with Dangerous Type vulnerability in Asghar Hatampoor BuddyPress Cover	N/A	A-BUD-BUDD-200624/312

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows Code Injection.This issue affects BuddyPress Cover: from n/a through 2.1.4.2. **CVE ID: CVE-2024-35746**		
Vendor: Cisco					
Product: finesse					
Affected Version(s): * Up to (excluding) 11.6\\(1\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	6.1	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct a stored XSS attack by exploiting an RFI vulnerability. This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-rfi-Um7wT8Ew	A-CIS-FINE-200624/313

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected interface or access sensitive information on the affected device. **CVE ID: CVE-2024-20405**		
Server-Side Request Forgery (SSRF)	05-Jun-2024	5.3	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct an SSRF attack on an affected system. This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated to the affected device. **CVE ID: CVE-2024-20404**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-rfi-Um7wT8Ew	A-CIS-FINE-200624/314

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 11.6\\(1\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	6.1	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct a stored XSS attack by exploiting an RFI vulnerability. This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive information on the affected device. **CVE ID: CVE-2024-20405**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-rfi-Um7wT8Ew	A-CIS-FINE-200624/315
Server-Side Request	05-Jun-2024	5.3	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com/security/cente	A-CIS-FINE-200624/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct an SSRF attack on an affected system. This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated to the affected device. **CVE ID: CVE-2024-20404**	r/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-rfi-Um7wT8Ew	
Affected Version(s): 12.6\\(2\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	6.1	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-rfi-Um7wT8Ew	A-CIS-FINE-200624/317

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conduct a stored XSS attack by exploiting an RFI vulnerability. This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive information on the affected device. **CVE ID: CVE-2024-20405**		
Server-Side Request Forgery (SSRF)	05-Jun-2024	5.3	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct an SSRF attack on an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-rfi-Um7wT8Ew	A-CIS-FINE-200624/318

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated to the affected device. **CVE ID: CVE-2024-20404**		
Vendor: clashforwindows					
Product: clash					
Affected Version(s): From (including) 0.1.0 Up to (including) 0.20.1					
Improper Authentication	07-Jun-2024	9.8	A vulnerability was found in Clash up to 0.20.1 on Windows. It has been declared as critical. This vulnerability affects unknown code of the component Proxy Port. The manipulation leads to improper authentication. The attack can be initiated remotely.	N/A	A-CLA-CLAS-200624/319

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. It is recommended to change the configuration settings. VDB-267406 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-5732**		
Vendor: cloudfoundry					
Product: cf-deployment					
Affected Version(s): From (including) 30.9.0 Up to (including) 40.13.0					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	10-Jun-2024	7.5	Improper handling of requests in Routing Release > v0.273.0 and <= v0.297.0 allows an unauthenticated attacker to degrade the service availability of the Cloud Foundry deployment if performed at scale. **CVE ID: CVE-2024-22279**	https://www.cloudfoundry.org/blog/cve-2024-22279-gorouter-denial-of-service-attack/	A-CLO-CF-D-200624/320
Product: routing_release					
Affected Version(s): From (including) 0.273.0 Up to (including) 0.297.0					
Inconsistent Interpretation of HTTP Requests ('HTTP	10-Jun-2024	7.5	Improper handling of requests in Routing Release > v0.273.0 and <= v0.297.0 allows an unauthenticated attacker to degrade	https://www.cloudfoundry.org/blog/cve-2024-22279-gorouter-denial-of-service-attack/	A-CLO-ROUT-200624/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Request Smuggling')			the service availability of the Cloud Foundry deployment if performed at scale. **CVE ID: CVE-2024-22279**		
Vendor: Clusterlabs					
Product: booth					
Affected Version(s): * Up to (excluding) 1.1					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	A-CLU-BOOT-200624/322
Vendor: codeless					
Product: cowidgets_-_elementor					
Affected Version(s): * Up to (including) 1.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Codeless Cowidgets – Elementor Addons allows Stored XSS.This issue affects Cowidgets – Elementor Addons:	N/A	A-COD-COWI-200624/323

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from n/a through 1.1.1. **CVE ID: CVE-2024-35782**		
Vendor: codeparrots					
Product: easy_forms_for_mailchimp					
Affected Version(s): * Up to (including) 6.9.0					
Insertion of Sensitive Information into Log File	04-Jun-2024	7.5	Insertion of Sensitive Information into Log File vulnerability in Code Parrots Easy Forms for Mailchimp.This issue affects Easy Forms for Mailchimp: from n/a through 6.9.0. **CVE ID: CVE-2024-25095**	N/A	A-COD-EASY-200624/324
Missing Authorization	10-Jun-2024	7.3	Missing Authorization vulnerability in Code Parrots Easy Forms for Mailchimp.This issue affects Easy Forms for Mailchimp: from n/a through 6.9.0. **CVE ID: CVE-2024-35742**	N/A	A-COD-EASY-200624/325
Vendor: Codepeople					
Product: wp_time_slots_booking_form					
Affected Version(s): * Up to (excluding) 1.2.12					
Missing Authorization	10-Jun-2024	9.8	Missing Authorization vulnerability in CodePeople WP	N/A	A-COD-WP_T-200624/326

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Time Slots Booking Form.This issue affects WP Time Slots Booking Form: from n/a through 1.2.11. **CVE ID: CVE-2024-35735**		
Vendor: contact_form_builder_project					
Product: contact_form_builder					
Affected Version(s): * Up to (including) 2.1.7					
Improper Restriction of Excessive Authentication Attempts	10-Jun-2024	5.3	Improper Restriction of Excessive Authentication Attempts vulnerability in wpdevart Contact Form Builder, Contact Widget allows Functionality Bypass.This issue affects Contact Form Builder, Contact Widget: from n/a through 2.1.7. **CVE ID: CVE-2024-35747**	N/A	A-CON-CONT-200624/327
Vendor: creativethemes					
Product: blocksy					
Affected Version(s): * Up to (excluding) 2.0.51					
Improper Neutralization of Input During Web Page Generation	05-Jun-2024	5.4	The Blocksy theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the custom_url parameter in all	https://themes.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=229705%40blocks	A-CRE-BLOC-200624/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			versions up to, and including, 2.0.50 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-5439**	y%2F2.0.51&old=228990%40blocksy%2F2.0.50	
Vendor: crmeb					
Product: crmeb					
Affected Version(s): 5.2.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jun-2024	7.5	SQL Injection vulnerability in CRMEB v.5.2.2 allows a remote attacker to obtain sensitive information via the getProductList function in the ProductController.php file. **CVE ID: CVE-2024-36837**	N/A	A-CRM-CRME-200624/329
Vendor: cyberchimps					
Product: responsive					
Affected Version(s): * Up to (excluding) 5.0.3.1					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CyberChimps Responsive allows Stored XSS.This issue affects Responsive: from n/a through 5.0.3. **CVE ID: CVE-2024-35654**	N/A	A-CYB-RESP-200624/330
Product: responsive_addons					
Affected Version(s): * Up to (excluding) 3.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Responsive Addons – Starter Templates, Advanced Features and Customizer Settings for Responsive Theme. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 3.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web	https://plugins.trac.wordpress.org/changeset/3094256/responsive-add-ons/trunk/includes/importers/wxr-importer/class-responsive-ready-sites-wxr-importer.php	A-CYB-RESP-200624/331

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5222**		
Vendor: cyrusimap					
Product: cyrus_imap					
Affected Version(s): * Up to (excluding) 3.8.3					
Allocation of Resources Without Limits or Throttling	05-Jun-2024	6.5	Cyrus IMAP before 3.8.3 and 3.10.x before 3.10.0-rc1 allows authenticated attackers to cause unbounded memory allocation by sending many LITERALs in a single command. **CVE ID: CVE-2024-34055**	https://github.com/cyrusimap/cyrus-imapd/commit/ef9e4e8314d6a06f2269af0ccf606894cc3fe489	A-CYR-CYRU-200624/332
Affected Version(s): 3.10.0					
Allocation of Resources Without Limits or Throttling	05-Jun-2024	6.5	Cyrus IMAP before 3.8.3 and 3.10.x before 3.10.0-rc1 allows authenticated attackers to cause unbounded memory allocation by sending many LITERALs in a single command. **CVE ID: CVE-2024-34055**	https://github.com/cyrusimap/cyrus-imapd/commit/ef9e4e8314d6a06f2269af0ccf606894cc3fe489	A-CYR-CYRU-200624/333
Vendor: dextaz_ping_project					
Product: dextaz_ping					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 0.65					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Jun-2024	7.2	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in dexta Dextaz Ping allows Command Injection.This issue affects Dextaz Ping: from n/a through 0.65. **CVE ID: CVE-2024-34792**	N/A	A-DEX-DEXT-200624/334
Vendor: dreryk					
Product: gabinet					
Affected Version(s): From (including) 7.0.0.0 Up to (excluding) 9.17.0.0					
Use of Hard-coded Credentials	10-Jun-2024	9.8	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among all drEryk Gabinet installations.This issue affects drEryk Gabinet software versions from 7.0.0.0 through 9.17.0.0. **CVE ID: CVE-2024-3699**	N/A	A-DRE-GABI-200624/335
Vendor: dulldusk					
Product: phpfilemanager					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.7.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-2024	6.1	Vulnerability in Dulldusk's PHP File Manager affecting version 1.7.8. This vulnerability consists of an XSS through the fm_current_dir parameter of index.php. An attacker could send a specially crafted JavaScript payload to an authenticated user and partially hijack their browser session. **CVE ID: CVE-2024-5673**	N/A	A-DUL-PHPF-200624/336
Vendor: elearningfreak					
Product: insert_or_embed_articulate_content					
Affected Version(s): * Up to (including) 4.3000000023					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	5.4	The Insert or Embed Articulate Content into WordPress plugin through 4.3000000023 lacks validation of URLs when adding iframes, allowing attackers to inject an iFrame in the page and thus load arbitrary content from any page. **CVE ID: CVE-2024-0756**	N/A	A-ELE-INSE-200624/337
Vendor: emailgpt					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: emailgpt					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jun-2024	9.1	The EmailGPT service contains a prompt injection vulnerability. The service uses an API service that allows a malicious user to inject a direct prompt and take over the service logic. Attackers can exploit the issue by forcing the AI service to leak the standard hard-coded system prompts and/or execute unwanted prompts. When engaging with EmailGPT by submitting a malicious prompt that requests harmful information, the system will respond by providing the requested data. This vulnerability can be exploited by any individual with access to the service. **CVE ID: CVE-2024-5184**	N/A	A-EMA-EMAI-200624/338
Vendor: emlog					
Product: emlog					
Affected Version(s): 2.3.0					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	10-Jun-2024	6.5	Emlog pro2.3 is vulnerable to Cross Site Request Forgery (CSRF) via twitter.php which can be used with a XSS vulnerability to access administrator information. **CVE ID: CVE-2024-31612**	N/A	A-EML-EMLO-200624/339
Vendor: envothemes					
Product: envo_extra					
Affected Version(s): * Up to (excluding) 1.8.25					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	5.4	The Envo Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button_css_id' parameter within the Button widget in all versions up to, and including, 1.8.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	https://plugins.trac.wordpress.org/changeset/3098500/	A-ENV-ENVO-200624/340

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-5645		
Vendor: envoyproxy					
Product: envoy					
Affected Version(s): * Up to (excluding) 1.27.6					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Jun-2024	8.2	Envoy is a cloud-native, open source edge and service proxy. A theoretical request smuggling vulnerability exists through Envoy if a server can be tricked into adding an upgrade header into a response. Per RFC https://www.rfc-editor.org/rfc/rfc7230#section-6.7 a server sends 101 when switching protocols. Envoy incorrectly accepts a 200 response from a server when requesting a protocol upgrade, but 200 does not indicate protocol switch. This opens up the possibility of request smuggling through Envoy if the server can be tricked into adding the upgrade header to the response.	https://github.com/envoyproxy/envoy/security/advisories/GHSA-vcf8-7238-v74c	A-ENV-ENVO-200624/341

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23326		
Use After Free	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. A crash was observed in `EnvoyQuicServerStream::OnInitialHeadersComplete()` with following call stack. It is a use-after-free caused by QUICHE continuing push request headers after `StopReading()` being called on the stream. As after `StopReading()`, the HCM's `ActiveStream` might have already be destroyed and any up calls from QUICHE could potentially cause use after free. **CVE ID: CVE-2024-32974**	N/A	A-ENV-ENVO-200624/342
Integer Underflow (Wrap or Wraparound)	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. There is a crash at `QuicheDataReader::PeekVarInt62Length()`. It is caused by integer underflow in the `QuicStreamSequencerBuffer::PeekRe	N/A	A-ENV-ENVO-200624/343

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gion()` implementation. **CVE ID: CVE-2024-32975**		
Out-of-bounds Write	04-Jun-2024	6.5	Envoy is a cloud-native, open source edge and service proxy. Envoy exposed an out-of-memory (OOM) vector from the mirror response, since async HTTP client will buffer the response with an unbounded buffer. **CVE ID: CVE-2024-34364**	N/A	A-ENV-ENVO-200624/344
Use After Free	04-Jun-2024	5.9	Envoy is a cloud-native, open source edge and service proxy. There is a use-after-free in `HttpConnectionManager` (HCM) with `EnvoyQuicServerStream` that can crash Envoy. An attacker can exploit this vulnerability by sending a request without `FIN`, then a `RESET_STREAM` frame, and then after receiving the response, closing the connection. **CVE ID: CVE-2024-34362**	N/A	A-ENV-ENVO-200624/345
Affected Version(s): From (including) 1.18.0 Up to (excluding) 1.27.6					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. Envoyproxy with a Brotli filter can get into an endless loop during decompression of Brotli data with extra input. **CVE ID: CVE-2024-32976**	N/A	A-ENV-ENVO-200624/346
Affected Version(s): From (including) 1.28.0 Up to (excluding) 1.28.4					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Jun-2024	8.2	Envoy is a cloud-native, open source edge and service proxy. A theoretical request smuggling vulnerability exists through Envoy if a server can be tricked into adding an upgrade header into a response. Per RFC https://www.rfc-editor.org/rfc/rfc7230#section-6.7 a server sends 101 when switching protocols. Envoy incorrectly accepts a 200 response from a server when requesting a protocol upgrade, but 200 does not indicate protocol switch. This opens up the possibility of request smuggling through Envoy if the server can be	https://github.com/envoyproxy/envoy/security/advisories/GHSA-vcf8-7238-v74c	A-ENV-ENVO-200624/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tricked into adding the upgrade header to the response. **CVE ID: CVE-2024-23326**		
Use After Free	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. A crash was observed in `EnvoyQuicServerStream::OnInitialHeadersComplete()` with following call stack. It is a use-after-free caused by QUICHE continuing push request headers after `StopReading()` being called on the stream. As after `StopReading()`, the HCM's `ActiveStream` might have already be destroyed and any up calls from QUICHE could potentially cause use after free. **CVE ID: CVE-2024-32974**	N/A	A-ENV-ENVO-200624/348
Integer Underflow (Wrap or Wraparound)	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. There is a crash at `QuicheDataReader	N/A	A-ENV-ENVO-200624/349

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			::PeekVarInt62Length()`. It is caused by integer underflow in the `QuicStreamSequencerBuffer::PeekRegion()` implementation. **CVE ID: CVE-2024-32975**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. Envoyproxy with a Brotli filter can get into an endless loop during decompression of Brotli data with extra input. **CVE ID: CVE-2024-32976**	N/A	A-ENV-ENVO-200624/350
N/A	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. Due to how Envoy invoked the nlohmann JSON library, the library could throw an uncaught exception from downstream data if incomplete UTF-8 strings were serialized. The uncaught exception would cause Envoy to crash. **CVE ID: CVE-2024-34363**	N/A	A-ENV-ENVO-200624/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jun-2024	6.5	Envoy is a cloud-native, open source edge and service proxy. Envoy exposed an out-of-memory (OOM) vector from the mirror response, since async HTTP client will buffer the response with an unbounded buffer. **CVE ID: CVE-2024-34364**	N/A	A-ENV-ENVO-200624/352
Use After Free	04-Jun-2024	5.9	Envoy is a cloud-native, open source edge and service proxy. There is a use-after-free in `HttpConnectionManager` (HCM) with `EnvoyQuicServerStream` that can crash Envoy. An attacker can exploit this vulnerability by sending a request without `FIN`, then a `RESET_STREAM` frame, and then after receiving the response, closing the connection. **CVE ID: CVE-2024-34362**	N/A	A-ENV-ENVO-200624/353
Affected Version(s): From (including) 1.29.0 Up to (excluding) 1.29.5					
Inconsistent Interpretation of	04-Jun-2024	8.2	Envoy is a cloud-native, open source edge and service proxy. A theoretical	https://github.com/envoyproxy/envoy/security/advisories/GH	A-ENV-ENVO-200624/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
HTTP Requests ('HTTP Request Smuggling')			request smuggling vulnerability exists through Envoy if a server can be tricked into adding an upgrade header into a response. Per RFC https://www.rfc-editor.org/rfc/rfc7230#section-6.7 a server sends 101 when switching protocols. Envoy incorrectly accepts a 200 response from a server when requesting a protocol upgrade, but 200 does not indicate protocol switch. This opens up the possibility of request smuggling through Envoy if the server can be tricked into adding the upgrade header to the response. **CVE ID: CVE-2024-23326**	SA-vcf8-7238-v74c	
Use After Free	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. A crash was observed in `EnvoyQuicServerStream::OnInitialHeadersComplete()` with following call stack. It is a use-	N/A	A-ENV-ENVO-200624/355

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after-free caused by QUICHE continuing push request headers after `StopReading()` being called on the stream. As after `StopReading()`, the HCM's `ActiveStream` might have already be destroyed and any up calls from QUICHE could potentially cause use after free. **CVE ID: CVE-2024-32974**		
Integer Underflow (Wrap or Wraparound)	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. There is a crash at `QuicheDataReader::PeekVarInt62Length()`. It is caused by integer underflow in the `QuicStreamSequencerBuffer::PeekRegion()` implementation. **CVE ID: CVE-2024-32975**	N/A	A-ENV-ENVO-200624/356
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. Envoyproxy with a Brotli filter can get into an endless loop during	N/A	A-ENV-ENVO-200624/357

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decompression of Brotli data with extra input. **CVE ID: CVE-2024-32976**		
N/A	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. Due to how Envoy invoked the nlohmann JSON library, the library could throw an uncaught exception from downstream data if incomplete UTF-8 strings were serialized. The uncaught exception would cause Envoy to crash. **CVE ID: CVE-2024-34363**	N/A	A-ENV-ENVO-200624/358
Out-of-bounds Write	04-Jun-2024	6.5	Envoy is a cloud-native, open source edge and service proxy. Envoy exposed an out-of-memory (OOM) vector from the mirror response, since async HTTP client will buffer the response with an unbounded buffer. **CVE ID: CVE-2024-34364**	N/A	A-ENV-ENVO-200624/359
Use After Free	04-Jun-2024	5.9	Envoy is a cloud-native, open source edge and service proxy. There is a	N/A	A-ENV-ENVO-200624/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use-after-free in `HttpConnectionManager` (HCM) with `EnvoyQuicServerStream` that can crash Envoy. An attacker can exploit this vulnerability by sending a request without `FIN`, then a `RESET_STREAM` frame, and then after receiving the response, closing the connection. **CVE ID: CVE-2024-34362**		
Affected Version(s): From (including) 1.30.0 Up to (excluding) 1.30.2					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Jun-2024	8.2	Envoy is a cloud-native, open source edge and service proxy. A theoretical request smuggling vulnerability exists through Envoy if a server can be tricked into adding an upgrade header into a response. Per RFC https://www.rfc-editor.org/rfc/rfc7230#section-6.7 a server sends 101 when switching protocols. Envoy incorrectly accepts a 200 response from a server when requesting a protocol upgrade, but 200 does not	https://github.com/envoyproxy/envoy/security/advisories/GHSA-vcf8-7238-v74c	A-ENV-ENVO-200624/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			indicate protocol switch. This opens up the possibility of request smuggling through Envoy if the server can be tricked into adding the upgrade header to the response. **CVE ID: CVE-2024-23326**		
Use After Free	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. A crash was observed in `EnvoyQuicServerStream::OnInitialHeadersComplete()` with following call stack. It is a use-after-free caused by QUICHE continuing push request headers after `StopReading()` being called on the stream. As after `StopReading()`, the HCM's `ActiveStream` might have already be destroyed and any up calls from QUICHE could potentially cause use after free. **CVE ID: CVE-2024-32974**	N/A	A-ENV-ENVO-200624/362

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. There is a crash at `QuicheDataReader::PeekVarInt62Length()`. It is caused by integer underflow in the `QuicStreamSequencerBuffer::PeekRegion()` implementation. **CVE ID: CVE-2024-32975**	N/A	A-ENV-ENVO-200624/363
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. Envoyproxy with a Brotli filter can get into an endless loop during decompression of Brotli data with extra input. **CVE ID: CVE-2024-32976**	N/A	A-ENV-ENVO-200624/364
N/A	04-Jun-2024	7.5	Envoy is a cloud-native, open source edge and service proxy. Due to how Envoy invoked the nlohmann JSON library, the library could throw an uncaught exception from downstream data if incomplete UTF-8 strings were serialized. The uncaught exception	N/A	A-ENV-ENVO-200624/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would cause Envoy to crash. **CVE ID: CVE-2024-34363**		
Out-of-bounds Write	04-Jun-2024	6.5	Envoy is a cloud-native, open source edge and service proxy. Envoy exposed an out-of-memory (OOM) vector from the mirror response, since async HTTP client will buffer the response with an unbounded buffer. **CVE ID: CVE-2024-34364**	N/A	A-ENV-ENVO-200624/366
Use After Free	04-Jun-2024	5.9	Envoy is a cloud-native, open source edge and service proxy. There is a use-after-free in `HttpConnectionManager` (HCM) with `EnvoyQuicServerStream` that can crash Envoy. An attacker can exploit this vulnerability by sending a request without `FIN`, then a `RESET_STREAM` frame, and then after receiving the response, closing the connection. **CVE ID: CVE-2024-34362**	N/A	A-ENV-ENVO-200624/367
Vendor: estomed					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: simple_care					
Affected Version(s): *					
Use of Hard-coded Credentials	10-Jun-2024	9.8	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among all Simple Care software installations. This issue affects Estomed Sp. z o.o. Simple Care software in all versions. The software is no longer supported. **CVE ID: CVE-2024-3700**	N/A	A-EST-SIMP-200624/368
Vendor: eurosoft					
Product: przychodnia					
Affected Version(s): * Up to (excluding) 20240417.001					
Use of Hard-coded Credentials	10-Jun-2024	9.8	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among all Eurosoft Przychodnia installations.	N/A	A-EUR-PRZY-200624/369

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Eurosoft Przychodnia software before version 20240417.001 (from that version vulnerability is fixed). **CVE ID: CVE-2024-1228**		
Vendor: extendthemes					
Product: colibri_page_builder					
Affected Version(s): * Up to (excluding) 1.0.277					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-2024	5.4	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.0.276 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	https://plugins.trac.wordpress.org/changeset/3097694/	A-EXT-COLI-200624/370

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-5038		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	5.4	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's colibri_video_player shortcode in all versions up to, and including, 1.0.276 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-4451**	https://plugins.trac.wordpress.org/changeset/3097694/colibri-page-builder/trunk/extend-builder/shortcodes/video.php	A-EXT-COLI-200624/371
Vendor: fileorganizer					
Product: fileorganizer					
Affected Version(s): * Up to (excluding) 1.0.8					
N/A	07-Jun-2024	7.5	The FileOrganizer – Manage WordPress and Website Files plugin for WordPress is vulnerable to Sensitive	https://plugins.trac.wordpress.org/changeset/3098763/	A-FIL-FILE-200624/372

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information Exposure in all versions up to, and including, 1.0.7 via the 'fileorganizer_ajax_handler' function. This makes it possible for unauthenticated attackers to extract sensitive data including backups or other sensitive information if the files have been moved to the built-in Trash folder. **CVE ID: CVE-2024-5599**		
Vendor: fivestarplugins					
Product: five_star_restaurant_menu					
Affected Version(s): * Up to (excluding) 2.4.17					
Missing Authorization	05-Jun-2024	4.3	The Restaurant Menu and Food Ordering plugin for WordPress is vulnerable to unauthorized creation of data due to a missing capability check on 'add_section', 'add_menu', 'add_menu_item', and 'add_menu_page' functions in all versions up to, and including, 2.4.16. This makes it possible for	https://plugins.trac.wordpress.org/changeset/3097599/	A-FIV-FIVE-200624/373

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attackers, with Subscriber-level access and above, to create menu sections, menus, food items, and new menu pages. **CVE ID: CVE-2024-5459**		
Vendor: formwork_project					
Product: formwork					
Affected Version(s): * Up to (excluding) 1.13.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	4.8	Formwork is a flat file-based Content Management System (CMS). An attackers (requires administrator privilege) to execute arbitrary web scripts by modifying site options via /panel/options/site. This type of attack is suitable for persistence, affecting visitors across all pages (except the dashboard). This vulnerability is fixed in 1.13.1. **CVE ID: CVE-2024-37160**	https://github.com/getformwork/formwork/commit/9d471204f7ebb51c3c27131581c2b834315b5e0b, https://github.com/getformwork/formwork/commit/f5312015a5a5e89b95ef2bd07e496f8474d579c5	A-FOR-FORM-200624/374
Vendor: Fortinet					
Product: fortiwebmanager					
Affected Version(s): 6.0.2					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	05-Jun-2024	8.8	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. **CVE ID: CVE-2024-23669**	https://fortiguard.fortinet.com/psirt/FG-IR-23-222	A-FOR-FORT-200624/375
Affected Version(s): 6.3.0					
Incorrect Authorization	05-Jun-2024	8.8	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. **CVE ID: CVE-2024-23669**	https://fortiguard.fortinet.com/psirt/FG-IR-23-222	A-FOR-FORT-200624/376
Affected Version(s): 7.2.0					
Incorrect Authorization	05-Jun-2024	8.8	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and	https://fortiguard.fortinet.com/psirt/FG-IR-23-222	A-FOR-FORT-200624/377

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. **CVE ID: CVE-2024-23669**		
Affected Version(s): From (including) 6.2.3 Up to (excluding) 6.2.5					
Incorrect Authorization	05-Jun-2024	8.8	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. **CVE ID: CVE-2024-23669**	https://fortiguard.fortinet.com/psirt/FG-IR-23-222	A-FOR-FORT-200624/378
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.5					
Incorrect Authorization	05-Jun-2024	8.8	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI.	https://fortiguard.fortinet.com/psirt/FG-IR-23-222	A-FOR-FORT-200624/379

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23669		
Vendor: fujielectric					
Product: monitouch_v-sft					
Affected Version(s): * Up to (excluding) 6.2.3.0					
Access of Resource Using Incompatible Type ('Type Confusion')	10-Jun-2024	9.8	Fuji Electric Monitouch V-SFT is vulnerable to a type confusion, which could cause a crash or code execution. **CVE ID: CVE-2024-5597**	N/A	A-FUJ-MONI-200624/380
Vendor: gaizhenbiao					
Product: chuanhuchatgpt					
Affected Version(s): * Up to (including) 20240410					
N/A	04-Jun-2024	7.5	An improper access control vulnerability exists in the gaizhenbiao/chuanhuchatgpt application, specifically in version 20240410. This vulnerability allows any user on the server to access the chat history of any other user without requiring any form of interaction between the users. Exploitation of this vulnerability could lead to data breaches, including the exposure of sensitive personal details, financial	N/A	A-GAI-CHUA-200624/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data, or confidential conversations. Additionally, it could facilitate identity theft and manipulation or fraud through the unauthorized access to users' chat histories. This issue is due to insufficient access control mechanisms in the application's handling of chat history data. **CVE ID: CVE-2024-4520**		
Vendor: gamipress					
Product: gamipress_-_link					
Affected Version(s): * Up to (excluding) 1.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The GamiPress – Link plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's gamipress_link shortcode in all versions up to, and including, 1.1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3096646%40gamipress-link%2Ftrunk&old=2989725%40gamipress-link%2Ftrunk&sfp_email=&sfph_mail=	A-GAM-GAMI-200624/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5536**		
Vendor: generatepress					
Product: generatepress					
Affected Version(s): * Up to (excluding) 2.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	6.1	The GP Premium plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the message parameter in all versions up to, and including, 2.4.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-3469**	N/A	A-GEN-GENE-200624/383
Vendor: getawesomesupport					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: awesome_support					
Affected Version(s): * Up to (excluding) 6.1.8					
Missing Authorization	10-Jun-2024	8.8	Missing Authorization vulnerability in Awesome Support Team Awesome Support.This issue affects Awesome Support: from n/a through 6.1.7. **CVE ID: CVE-2024-35741**	N/A	A-GET-AWES-200624/384
Vendor: getbrave					
Product: brave					
Affected Version(s): * Up to (including) 0.6.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brave Brave Popup Builder allows Stored XSS.This issue affects Brave Popup Builder: from n/a through 0.6.9. **CVE ID: CVE-2024-35655**	N/A	A-GET-BRAV-200624/385
Vendor: getshortcodes					
Product: shortcodes_ultimate					
Affected Version(s): * Up to (excluding) 7.1.7					
Improper Neutralization of Input During Web Page	05-Jun-2024	5.4	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&repon	A-GET-SHOR-200624/386

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			vulnerable to Stored Cross-Site Scripting via the plugin's su_lightbox shortcode in all versions up to, and including, 7.1.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-4821**	ame=&new=3096024%40shortcodes-ultimate%2Ftrunk&old=3084162%40shortcodes-ultimate%2Ftrunk&sfp_email=&sfph_mail=#file1	
Vendor: Golang					
Product: go					
Affected Version(s): * Up to (excluding) 1.21.11					
N/A	05-Jun-2024	9.8	The various Is methods (IsPrivate, IsLoopback, etc) did not work as expected for IPv4-mapped IPv6 addresses, returning false for addresses which would return true in their traditional IPv4 forms. **CVE ID: CVE-2024-24790**	https://go.dev/cl/590316	A-GOL-GO-200624/387

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jun-2024	5.5	The archive/zip package's handling of certain types of invalid zip files differs from the behavior of most zip implementations. This misalignment could be exploited to create an zip file with contents that vary depending on the implementation reading the file. The archive/zip package now rejects files containing these errors. **CVE ID: CVE-2024-24789**	https://go.dev/cl/585397, https://go.dev/issue/66869	A-GOL-GO-200624/388
Affected Version(s): From (including) 1.22.0 Up to (excluding) 1.22.4					
N/A	05-Jun-2024	9.8	The various Is methods (IsPrivate, IsLoopback, etc) did not work as expected for IPv4-mapped IPv6 addresses, returning false for addresses which would return true in their traditional IPv4 forms. **CVE ID: CVE-2024-24790**	https://go.dev/cl/590316	A-GOL-GO-200624/389
N/A	05-Jun-2024	5.5	The archive/zip package's handling of certain types of invalid zip files differs from the	https://go.dev/cl/585397, https://go.dev/issue/66869	A-GOL-GO-200624/390

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior of most zip implementations. This misalignment could be exploited to create an zip file with contents that vary depending on the implementation reading the file. The archive/zip package now rejects files containing these errors. **CVE ID: CVE-2024-24789**		
Vendor: grafana					
Product: oncall					
Affected Version(s): From (including) 1.1.37 Up to (excluding) 1.5.2					
Server-Side Request Forgery (SSRF)	05-Jun-2024	9.1	Grafana OnCall is an easy-to-use on-call management tool that will help reduce toil in on-call management through simpler workflows and interfaces that are tailored specifically for engineers. Grafana OnCall, from version 1.1.37 before 1.5.2 are vulnerable to a Server Side Request Forgery (SSRF) vulnerability in the	https://grafana.com/security/security-advisories/cve-2024-5526/	A-GRA-ONCA-200624/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webhook functionallity. This issue was fixed in version 1.5.2 **CVE ID: CVE-2024-5526**		
Vendor: homebrew					
Product: jan					
Affected Version(s): 0.4.12					
Unrestricted Upload of File with Dangerous Type	04-Jun-2024	9.8	An arbitrary file upload vulnerability in the /v1/app/writeFileSync interface of Jan v0.4.12 allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID: CVE-2024-36858**	N/A	A-HOM-JAN-200624/392
Unrestricted Upload of File with Dangerous Type	04-Jun-2024	9.8	An arbitrary file upload vulnerability in the /v1/app/appendFileSync interface of Jan v0.4.12 allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID: CVE-2024-37273**	N/A	A-HOM-JAN-200624/393
N/A	04-Jun-2024	7.5	Jan v0.4.12 was discovered to contain an arbitrary file read vulnerability via the	N/A	A-HOM-JAN-200624/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/v1/app/readFileSync interface. **CVE ID: CVE-2024-36857**		
Vendor: horea_radu					
Product: one_page_express_companion					
Affected Version(s): * Up to (excluding) 1.6.38					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	5.4	The One Page Express Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's one_page_express_contact_form shortcode in all versions up to, and including, 1.6.37 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-4703**	https://plugins.trac.wordpress.org/changeset/3097699/one-page-express-companion	A-HOR-ONE_-200624/395
Vendor: icegram					
Product: email_subscribers_\&_newsletters					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.7.21					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jun-2024	9.8	The Email Subscribers by Icegram Express plugin for WordPress is vulnerable to SQL Injection via the 'hash' parameter in all versions up to, and including, 5.7.20 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-4295**	https://plugins.trac.wordpress.org/changeset/3090845/email-subscribers/trunk/lite/includes/db/class-es-db-lists-contacts.php	A-ICE-EMAI-200624/396
Vendor: idccms					
Product: idccms					
Affected Version(s): 1.35					
Cross-Site Request Forgery (CSRF)	04-Jun-2024	8.8	idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component	N/A	A-IDC-IDCC-200624/397

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin/vpsClass_deal.php?mudi=add **CVE ID: CVE-2024-36547**		
Cross-Site Request Forgery (CSRF)	04-Jun-2024	8.8	idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via admin/vpsCompany_deal.php?mudi=del **CVE ID: CVE-2024-36548**	N/A	A-IDC-IDCC-200624/398
Cross-Site Request Forgery (CSRF)	04-Jun-2024	8.8	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/vpsCompany_deal.php?mudi=rev&nohrefStr=close **CVE ID: CVE-2024-36549**	N/A	A-IDC-IDCC-200624/399
Cross-Site Request Forgery (CSRF)	04-Jun-2024	8.8	idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/vpsCompany_deal.php?mudi=add&nohrefStr=close **CVE ID: CVE-2024-36550**	N/A	A-IDC-IDCC-200624/400
Vendor: ipages_flipbook_project					
Product: ipages_flipbook					
Affected Version(s): * Up to (excluding) 1.5.2					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	10-Jun-2024	7.3	Missing Authorization vulnerability in Avirtum iPages Flipbook.This issue affects iPages Flipbook: from n/a through 1.5.1. **CVE ID: CVE-2024-4744**	N/A	A-IPA-IPAG-200624/401
Vendor: Jetbrains					
Product: aqua					
Affected Version(s): * Up to (excluding) 2024.1.2					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-AQUA-200624/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: clion					
Affected Version(s): * Up to (excluding) 2023.1.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-CLIO-200624/403

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.4					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-CLIO-200624/404

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.3.0 Up to (excluding) 2023.3.5					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-CLIO-200624/405

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.3					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-CLIO-200624/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: datagrip					
Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.4					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-DATA-200624/407

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.3.0 Up to (excluding) 2023.3.5					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-DATA-200624/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.1.0 Up to (excluding) 2023.1.3					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-DATA-200624/409

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.4					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-DATA-200624/410

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: dataspell					
Affected Version(s): * Up to (excluding) 2023.1.6					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-DATA-200624/411

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-DATA-200624/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.3.0 Up to (excluding) 2023.3.6					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-DATA-200624/413

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.2					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-DATA-200624/414

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: goland					
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.3					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-GOLA-200624/415

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): * Up to (excluding) 2023.1.6					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-GOLA-200624/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-GOLA-200624/417

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.3.0 Up to (excluding) 2023.3.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-GOLA-200624/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: intellij_idea					
Affected Version(s): * Up to (excluding) 2023.1.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-200624/419

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.3					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-200624/420

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-200624/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.3.0 Up to (excluding) 2023.3.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-200624/422

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: mps					
Affected Version(s): * Up to (excluding) 2023.2.1					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-MPS-200624/423

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): 2023.3.0					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-MPS-200624/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: phpstorm					
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.3					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-PHPS-200624/425

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): * Up to (excluding) 2023.1.6					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2;	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-PHPS-200624/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.3.0 Up to (excluding) 2023.3.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-PHPS-200624/427

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.6					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-PHPS-200624/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: pycharm					
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.3					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-PYCH-200624/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): * Up to (excluding) 2023.1.6					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-PYCH-200624/430

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.7					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-PYCH-200624/431

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.3.0 Up to (excluding) 2023.3.6					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-PYCH-200624/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: rider					
Affected Version(s): * Up to (excluding) 2023.1.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-RIDE-200624/433

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.3					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2;	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-RIDE-200624/434

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.3.0 Up to (excluding) 2023.3.6					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-RIDE-200624/435

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.5					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-RIDE-200624/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: rubymine					
Affected Version(s): * Up to (excluding) 2023.1.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-RUBY-200624/437

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.3					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-RUBY-200624/438

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.7					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-RUBY-200624/439

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.3.0 Up to (excluding) 2023.3.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-RUBY-200624/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: rustrover					
Affected Version(s): * Up to (excluding) 2024.1.1					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-RUST-200624/441

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Product: webstorm					
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.4					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-WEBS-200624/442

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): * Up to (excluding) 2023.1.6					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1;	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-WEBS-200624/443

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3,	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-WEBS-200624/444

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Affected Version(s): From (including) 2023.3.0 Up to (excluding) 2023.3.7					
Insufficiently Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-WEBS-200624/445

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 **CVE ID: CVE-2024-37051**		
Vendor: katello_project					
Product: katello					
Affected Version(s): -					
Improper Neutralization of Input	05-Jun-2024	4.8	A flaw was found in the Katello plugin for Foreman, where	N/A	A-KAT-KATE-200624/446

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			it is possible to store malicious JavaScript code in the "Description" field of a user. This code can be executed when opening certain pages, for example, Host Collections. **CVE ID: CVE-2024-4812**		
Vendor: la-studioweb					
Product: element_kit_for_elementor					
Affected Version(s): * Up to (excluding) 1.3.7.4					
Missing Authorization	10-Jun-2024	8.8	Missing Authorization vulnerability in LA-Studio LA-Studio Element Kit for Elementor.This issue affects LA-Studio Element Kit for Elementor: from n/a through 1.3.6. **CVE ID: CVE-2024-35725**	N/A	A-LA--ELEM-200624/447
Vendor: langflow					
Product: langflow					
Affected Version(s): * Up to (including) 0.6.19					
N/A	10-Jun-2024	9.8	Langflow through 0.6.19 allows remote code execution if untrusted users are able to reach the "POST /api/v1/custom_component" endpoint	N/A	A-LAN-LANG-200624/448

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and provide a Python script. **CVE ID: CVE-2024-37014**		
Vendor: lifterlms					
Product: lifterlms					
Affected Version(s): * Up to (excluding) 7.6.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jun-2024	6.5	The LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress is vulnerable to SQL Injection via the orderBy attribute of the lifterlms_favorites shortcode in all versions up to, and including, 7.6.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3095706%40lifterlms%2Ftrunk&old=3094820%40lifterlms%2Ftrunk&sfp_email=&sfph_mail=	A-LIF-LIFT-200624/449

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-4743		
Vendor: lunary					
Product: lunary					
Affected Version(s): 1.2.13					
N/A	09-Jun-2024	8.1	In lunary-ai/lunary version 1.2.13, an insufficient granularity of access control vulnerability allows users to create, update, get, and delete prompt variations for datasets not owned by their organization. This issue arises due to the application not properly validating the ownership of dataset prompts and their variations against the organization or project of the requesting user. As a result, unauthorized modifications to dataset prompts can occur, leading to altered or removed dataset prompts without proper authorization. This vulnerability impacts the integrity and consistency of dataset	N/A	A-LUN-LUNA-200624/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information, potentially affecting the results of experiments. **CVE ID: CVE-2024-5389**		
Vendor: lylme					
Product: lylme_spage					
Affected Version(s): 1.9.5					
Server-Side Request Forgery (SSRF)	04-Jun-2024	9.1	LyLme_spage v1.9.5 is vulnerable to Server-Side Request Forgery (SSRF) via the get_head function. **CVE ID: CVE-2024-36675**	N/A	A-LYL-LYLM-200624/451
Vendor: master-addons					
Product: master_addons					
Affected Version(s): * Up to (excluding) 2.0.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	6.1	The Master Addons – Free Widgets, Hover Effects, Toggle, Conditions, Animations for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Navigation Menu widget of the plugin's Mega Menu extension in all versions up to, and including, 2.0.6.1 due to insufficient input sanitization and output escaping on	https://plugins.trac.wordpress.org/changeset/3096299/master-addons	A-MAS-MAST-200624/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user supplied attributes. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5542**		
Missing Authorization	07-Jun-2024	5.3	The Master Addons – Free Widgets, Hover Effects, Toggle, Conditions, Animations for Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ma-template' REST API route in all versions up to, and including, 2.0.6.1. This makes it possible for unauthenticated attackers to create or modify existing Master Addons templates or make settings modifications related to these templates.	https://plugins.trac.wordpress.org/changeset/3096299/master-addons	A-MAS-MAST-200624/453

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-5382		
Vendor: melapress					
Product: melapress_login_security					
Affected Version(s): * Up to (excluding) 1.3.1					
Inclusion of Functionality from Untrusted Control Sphere	10-Jun-2024	7.2	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Melapress MelaPress Login Security allows PHP Remote File Inclusion.This issue affects MelaPress Login Security: from n/a through 1.3.0. **CVE ID: CVE-2024-35650**	N/A	A-MEL-MELA-200624/454
Vendor: meowapps					
Product: database_cleaner					
Affected Version(s): * Up to (excluding) 1.0.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	4.9	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Jordy Meow Database Cleaner allows Relative Path Traversal.This issue affects Database Cleaner:	N/A	A-MEO-DATA-200624/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from n/a through 1.0.5. **CVE ID: CVE-2024-35712**		
Vendor: metagauss					
Product: eventprime					
Affected Version(s): * Up to (excluding) 3.3.5					
Missing Authorization	09-Jun-2024	9.8	Missing Authorization vulnerability in Metagauss EventPrime.This issue affects EventPrime: from n/a through 3.3.4. **CVE ID: CVE-2024-31275**	N/A	A-MET-EVEN-200624/456
Product: profilegrid					
Affected Version(s): * Up to (excluding) 5.8.7					
Missing Authorization	05-Jun-2024	4.3	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pm_dismissible_notice and pm_wizard_update_group_icon functions in all versions up to, and including, 5.8.6. This makes it possible for authenticated	https://plugins.trac.wordpress.org/changeset/3095503/profilegrid-user-profiles-groups-and-communities/trunk/admin/class-profile-magic-admin.php?contextall=1	A-MET-PROF-200624/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers, with Subscriber-level access and above, to change arbitrary options to the value '1' or change group icons. **CVE ID: CVE-2024-5453**		
Vendor: mintplexlabs					
Product: anythingllm					
Affected Version(s): * Up to (including) 1.5.4					
Server-Side Request Forgery (SSRF)	05-Jun-2024	7.5	A Server-Side Request Forgery (SSRF) vulnerability exists in the latest version of mintplex-labs/anything-llm, allowing attackers to bypass the official fix intended to restrict access to intranet IP addresses and protocols. Despite efforts to filter out intranet IP addresses starting with 192, 172, 10, and 127 through regular expressions and limit access protocols to HTTP and HTTPS, attackers can still bypass these restrictions using alternative representations of IP addresses and accessing other	N/A	A-MIN-ANYT-200624/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ports running on localhost. This vulnerability enables attackers to access any asset on the internal network, attack web services on the internal network, scan hosts on the internal network, and potentially access AWS metadata endpoints. The vulnerability is due to insufficient validation of user-supplied URLs, which can be exploited to perform SSRF attacks. **CVE ID: CVE-2024-4084**		
Vendor: Mongodb					
Product: pymongo					
Affected Version(s): * Up to (excluding) 4.6.3					
Out-of-bounds Read	05-Jun-2024	8.1	An out-of-bounds read in the 'bson' module of PyMongo 4.6.2 or earlier allows deserialization of malformed BSON provided by a Server to raise an exception which may contain arbitrary application memory.	https://jira.mongodb.org/browse/PYTHON-4305	A-MON-PYMO-200624/459

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-5629		
Vendor: moveaddons					
Product: move_addons_for_elementor					
Affected Version(s): * Up to (excluding) 1.3.0					
Missing Authorization	04-Jun-2024	7.3	Missing Authorization vulnerability in moveaddons Move Addons for Elementor.This issue affects Move Addons for Elementor: from n/a through 1.2.9. **CVE ID: CVE-2024-30525**	N/A	A-MOV-MOVE-200624/460
Vendor: multivendorx					
Product: multivendorx					
Affected Version(s): * Up to (excluding) 4.1.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-2024	5.4	The MultiVendorX Marketplace – WooCommerce MultiVendor Marketplace Solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'hover_animation' parameter in all versions up to, and including, 4.1.11 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with	https://plugins.trac.wordpress.org/changeset/3097002/	A-MUL-MULT-200624/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5259**		
Affected Version(s): * Up to (excluding) 4.1.4					
Missing Authorization	09-Jun-2024	8.8	Missing Authorization vulnerability in MultiVendorX WC Marketplace.This issue affects WC Marketplace: from n/a through 4.1.3. **CVE ID: CVE-2024-31304**	N/A	A-MUL-MULT-200624/462
Vendor: netgsm					
Product: netgsm					
Affected Version(s): * Up to (including) 2.9.16					
Missing Authorization	04-Jun-2024	9.8	Missing Authorization vulnerability in Netgsm.This issue affects Netgsm: from n/a through 2.9.16. **CVE ID: CVE-2024-35672**	N/A	A-NET-NETG-200624/463
Missing Authorization	10-Jun-2024	6.3	Missing Authorization vulnerability in Netgsm.This issue affects Netgsm: from n/a through 2.9.16.	N/A	A-NET-NETG-200624/464

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-4746		
Vendor: netty					
Product: netty-incubator-codec-ohttp					
Affected Version(s): From (including) 0.0.3 Up to (excluding) 0.0.11					
Integer Overflow or Wraparound	04-Jun-2024	9.1	netty-incubator-codec-ohttp is the OHTTP implementation for netty. BoringSSLAEADContext keeps track of how many OHTTP responses have been sent and uses this sequence number to calculate the appropriate nonce to use with the encryption algorithm. Unfortunately, two separate errors combine which would allow an attacker to cause the sequence number to overflow and thus the nonce to repeat. **CVE ID: CVE-2024-36121**	https://github.com/netty/netty-incubator-codec-ohttp/security/advisories/GHSA-g762-h86w-8749	A-NET-NETT-200624/465
Vendor: online_discussion_forum_project					
Product: online_discussion_forum					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an	07-Jun-2024	9.8	A vulnerability was found in itsourcecode Online Discussion Forum 1.0. It has been rated as	N/A	A-ONL-ONLI-200624/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			critical. This issue affects some unknown processing of the file register_me.php. The manipulation of the argument eaddress leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-267407. **CVE ID: CVE-2024-5733**		
Unrestricted Upload of File with Dangerous Type	07-Jun-2024	8.8	A vulnerability classified as critical has been found in itsourcecode Online Discussion Forum 1.0. Affected is an unknown function of the file /members/poster.php. The manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be	N/A	A-ONL-ONLI-200624/467

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. The identifier of this vulnerability is VDB-267408. **CVE ID: CVE-2024-5734**		
Vendor: opentelemetry					
Product: configgrpc					
Affected Version(s): * Up to (excluding) 0.102.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Jun-2024	7.5	The OpenTelemetry Collector offers a vendor-agnostic implementation on how to receive, process and export telemetry data. An unsafe decompression vulnerability allows unauthenticated attackers to crash the collector via excessive memory consumption. OTel Collector version 0.102.1 fixes this issue. It is also fixed in the confighttp module version 0.102.0 and configgrpc module version 0.102.1. **CVE ID: CVE-2024-36129**	https://github.com/open-telemetry/opentelemetry-collector/pull/10289, https://github.com/open-telemetry/opentelemetry-collector/pull/10323, https://opentelemetry.io/blog/2024/cve-2024-36129	A-OPE-CONF-200624/468
Product: confighttp					
Affected Version(s): * Up to (excluding) 0.102.0					
Improper Restriction	05-Jun-2024	7.5	The OpenTelemetry	https://github.com/open-	A-OPE-CONF-200624/469

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Collector offers a vendor-agnostic implementation on how to receive, process and export telemetry data. An unsafe decompression vulnerability allows unauthenticated attackers to crash the collector via excessive memory consumption. OTel Collector version 0.102.1 fixes this issue. It is also fixed in the confighttp module version 0.102.0 and configgrpc module version 0.102.1. **CVE ID: CVE-2024-36129**	telemetry/opentelemetry-collector/pull/10289, https://github.com/open-telemetry/opentelemetry-collector/pull/10323, https://opentelemetry.io/blog/2024/cve-2024-36129	
Product: opentelemetry_collector					
Affected Version(s): * Up to (excluding) 0.102.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Jun-2024	7.5	The OpenTelemetry Collector offers a vendor-agnostic implementation on how to receive, process and export telemetry data. An unsafe decompression vulnerability allows unauthenticated attackers to crash	https://github.com/open-telemetry/opentelemetry-collector/pull/10289, https://github.com/open-telemetry/opentelemetry-collector/pull/10323, https://opentelemetry.io/blog/	A-OPE-OPEN-200624/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the collector via excessive memory consumption. OTel Collector version 0.102.1 fixes this issue. It is also fixed in the confighttp module version 0.102.0 and configgrpc module version 0.102.1. **CVE ID: CVE-2024-36129**	2024/cve-2024-36129	
Vendor: opmc					
Product: woocommerce_dropshipping					
Affected Version(s): * Up to (including) 5.0.4					
Missing Authorization	09-Jun-2024	5.3	Missing Authorization vulnerability in OPMC WooCommerce Dropshipping.This issue affects WooCommerce Dropshipping: from n/a through 5.0.4. **CVE ID: CVE-2024-35748**	N/A	A-OPM-WOOC-200624/471
Vendor: oretnom23					
Product: online_medicine_ordering_system					
Affected Version(s): 1.0					
N/A	10-Jun-2024	9.1	Sourcecodester Online Medicine Ordering System 1.0 is vulnerable to Arbitrary file deletion vulnerability as the backend settings	N/A	A-ORE-ONLI-200624/472

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have the function of deleting pictures to delete any files. **CVE ID: CVE-2024-32167**		
Vendor: ovic_importer_project					
Product: ovic_importer					
Affected Version(s): * Up to (including) 1.6.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	6.5	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ovic Team Ovic Importer allows Path Traversal.This issue affects Ovic Importer: from n/a through 1.6.3. **CVE ID: CVE-2024-35754**	N/A	A-OVI-OVIC-200624/473
Vendor: parisneo					
Product: lollms_web_ui					
Affected Version(s): 9.6					
Cross-Site Request Forgery (CSRF)	10-Jun-2024	8.1	A Cross-Site Request Forgery (CSRF) vulnerability exists in the clear_personality_files_list function of the parisneo/lollms-webui v9.6. The vulnerability arises from the use of a GET request to clear personality	N/A	A-PAR-LOLL-200624/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files list, which lacks proper CSRF protection. This flaw allows attackers to trick users into performing actions without their consent, such as deleting important files on the system. The issue is present in the application's handling of requests, making it susceptible to CSRF attacks that could lead to unauthorized actions being performed on behalf of the user. **CVE ID: CVE-2024-4328**		
Vendor: pdfcrowd					
Product: save_as_pdf_plugin					
Affected Version(s): * Up to (excluding) 3.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pdfcrowd Save as PDF plugin by Pdfcrowd allows Stored XSS.This issue affects Save as PDF plugin by Pdfcrowd: from n/a through 3.2.3.	N/A	A-PDF-SAVE-200624/475

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-35649		
Vendor: pharmacy\/medical_store_point_of_sale_system_project					
Product: pharmacy\/medical_store_point_of_sale_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-2024	9.8	Sourcecodester Pharmacy/Medical Store Point of Sale System 1.0 is vulnerable SQL Injection via login.php. This vulnerability stems from inadequate validation of user inputs for the email and password parameters, allowing attackers to inject malicious SQL queries. **CVE ID: CVE-2024-36673**	N/A	A-PHA-PHAR-200624/476
Vendor: PHP					
Product: php					
Affected Version(s): From (including) 5.0.0 Up to (excluding) 8.1.29					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Jun-2024	9.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line	N/A	A-PHP-PHP-200624/477

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. **CVE ID: CVE-2024-4577**		
Affected Version(s): From (including) 7.3.27 Up to (including) 7.3.33					
Insufficient Verification of Data Authenticity	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.	https://github.com/php/php-src/security/advisories/GHSA-w8qr-v226-r27w	A-PHP-PHP-200624/478

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-5458		
Affected Version(s): From (including) 7.4.15 Up to (including) 7.4.33					
Insufficient Verification of Data Authenticity	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. **CVE ID: CVE-2024-5458**	https://github.com/php/php-src/security/advisories/GHSA-w8qr-v226-r27w	A-PHP-PHP-200624/479
Affected Version(s): From (including) 8.0.2 Up to (including) 8.0.30					
Insufficient Verification of Data Authenticity	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VAL	https://github.com/php/php-src/security/advisories/GHSA-w8qr-v226-r27w	A-PHP-PHP-200624/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. **CVE ID: CVE-2024-5458**		
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.1.29					
Improper Encoding or Escaping of Output	09-Jun-2024	8.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874 does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary	N/A	A-PHP-PHP-200624/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands in Windows shell. **CVE ID: CVE-2024-5585**		
Observable Discrepancy	09-Jun-2024	5.9	The openssl_private_decrypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_PADDING, which is the default), is vulnerable to the Marvin Attack unless it is used with an OpenSSL version that includes the changes from this pull request: https://github.com/openssl/openssl/pull/13817 (rsa_pkcs1_implicit_rejection). These changes are part of OpenSSL 3.2 and have also been backported to stable versions of various Linux distributions, as well as to the PHP builds provided for Windows since the previous release. All distributors and builders should ensure that this version is used to prevent PHP from being vulnerable.	N/A	A-PHP-PHP-200624/482

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PHP Windows builds for the versions 8.1.29, 8.2.20 and 8.3.8 and above include OpenSSL patches that fix the vulnerability. **CVE ID: CVE-2024-2408**		
Insufficient Verification of Data Authenticity	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. **CVE ID: CVE-2024-5458**	https://github.com/php/php-src/security/advisories/GHSA-w8qr-v226-r27w	A-PHP-PHP-200624/483
Affected Version(s): From (including) 8.2.0 Up to (excluding) 8.2.20					
Improper Neutralization of	09-Jun-2024	9.8	In PHP versions 8.1.* before 8.1.29, 8.2.*	N/A	A-PHP-PHP-200624/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. **CVE ID: CVE-2024-4577**		
Improper Encoding or Escaping of Output	09-Jun-2024	8.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874 does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient	N/A	A-PHP-PHP-200624/485

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell. **CVE ID: CVE-2024-5585**		
Observable Discrepancy	09-Jun-2024	5.9	The openssl_private_decrypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_PADDING, which is the default), is vulnerable to the Marvin Attack unless it is used with an OpenSSL version that includes the changes from this pull request: https://github.com/openssl/openssl/pull/13817 (rsa_pkcs1_implicit_rejection). These changes are part of OpenSSL 3.2 and have also been backported to stable versions of various Linux distributions, as well as to the PHP builds provided for	N/A	A-PHP-PHP-200624/486

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows since the previous release. All distributors and builders should ensure that this version is used to prevent PHP from being vulnerable. PHP Windows builds for the versions 8.1.29, 8.2.20 and 8.3.8 and above include OpenSSL patches that fix the vulnerability. **CVE ID: CVE-2024-2408**		
Insufficient Verification of Data Authenticity	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and	https://github.com/php/php-src/security/advisories/GHSA-w8qr-v226-r27w	A-PHP-PHP-200624/487

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing them incorrectly. **CVE ID: CVE-2024-5458**		
Affected Version(s): From (including) 8.3.0 Up to (excluding) 8.3.8					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Jun-2024	9.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. **CVE ID: CVE-2024-4577**	N/A	A-PHP-PHP-200624/488
Improper Encoding or Escaping of Output	09-Jun-2024	8.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874	N/A	A-PHP-PHP-200624/489

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell. **CVE ID: CVE-2024-5585**		
Observable Discrepancy	09-Jun-2024	5.9	The openssl_private_decrypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_PADDING, which is the default), is vulnerable to the Marvin Attack unless it is used with an OpenSSL version that includes the changes from this pull request: https://github.com/openssl/openssl/pull/13817 (rsa_pkcs1_implicit_rejection). These	N/A	A-PHP-PHP-200624/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			changes are part of OpenSSL 3.2 and have also been backported to stable versions of various Linux distributions, as well as to the PHP builds provided for Windows since the previous release. All distributors and builders should ensure that this version is used to prevent PHP from being vulnerable. PHP Windows builds for the versions 8.1.29, 8.2.20 and 8.3.8 and above include OpenSSL patches that fix the vulnerability. **CVE ID: CVE-2024-2408**		
Insufficient Verification of Data Authenticity	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information	https://github.com/php/php-src/security/advisories/GHSA-w8qr-v226-r27w	A-PHP-PHP-200624/491

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. **CVE ID: CVE-2024-5458**		
Vendor: Pimcore					
Product: pimcore					
Affected Version(s): From (including) 11.0.0 Up to (excluding) 11.2.4					
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.5	Pimcore is an Open Source Data & Experience Management Platform. The Pimcore thumbnail generation can be used to flood the server with large files. By changing the file extension or scaling factor of the requested thumbnail, attackers can create files that are much larger in file size than the original. This vulnerability is fixed in 11.2.4. **CVE ID: CVE-2024-32871**	https://github.com/pimcore/pimcore/commit/38af70b3130f16fc27f2aea34e2943d7bdaaba06, https://github.com/pimcore/pimcore/commit/a6821a16ea38086bf6012e682e1743488244bd85, https://github.com/pimcore/pimcore/security/advisories/GHSA-277c-5vvj-9pwx	A-PIM-PIMC-200624/492
Vendor: porty					
Product: powerbank					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.02					
N/A	05-Jun-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in PORTY Smart Tech Technology Joint Stock Company PowerBank Application allows Retrieve Embedded Sensitive Data.This issue affects PowerBank Application: before 2.02. **CVE ID: CVE-2024-1662**	N/A	A-POR-POWE-200624/493
Vendor: pq-crystals					
Product: kyber					
Affected Version(s): * Up to (excluding) 2024-06-03					
Observable Discrepancy	10-Jun-2024	7.5	The Kyber reference implementation before 9b8d306, when compiled by LLVM Clang through 18.x with some common optimization options, has a timing side channel that allows attackers to recover an ML-KEM 512 secret key in minutes. This occurs because poly_frommsg in poly.c does not prevent Clang from	https://github.com/pq-crystals/kyber/commit/9b8d30698a3e7449aeb34e62339d4176f11e3c6c	A-PQ--KYBE-200624/494

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			emitting a vulnerable secret-dependent branch. **CVE ID: CVE-2024-37880**		
Vendor: projectdiscovery					
Product: interactsh					
Affected Version(s): From (including) 0.0.6 Up to (excluding) 1.2.0					
Files or Directories Accessible to External Parties	05-Jun-2024	9.8	Files or Directories Accessible to External Parties vulnerability in smb server in ProjectDiscovery Interactsh allows remote attackers to read/write any files in the directory and subdirectories of where the victim runs interactsh-server via anonymous login. **CVE ID: CVE-2024-5262**	https://github.com/projectdiscovery/interactsh/pull/874	A-PRO-INTE-200624/495
Vendor: purechat					
Product: pure_chat					
Affected Version(s): * Up to (excluding) 2.3					
Cross-Site Request Forgery (CSRF)	05-Jun-2024	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Pure Chat by Ruby Pure Chat.This issue affects Pure Chat: from n/a through 2.22. **CVE ID: CVE-2024-35673**	N/A	A-PUR-PURE-200624/496
Vendor: qodeinteractive					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qi_blocks					
Affected Version(s): * Up to (excluding) 1.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-2024	5.4	The Qi Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 1.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5221**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3097241%40qi-blocks%2Ftrunk&old=3094374%40qi-blocks%2Ftrunk&sfp_email=&sfph_mail=	A-QOD-QI_B-200624/497
Vendor: Redhat					
Product: openshift_container_platform					
Affected Version(s): 4.0					
Authentication Bypass by Spoofing	05-Jun-2024	7.5	A flaw was found in OpenShift's Telemeter. If certain conditions are in place, an attacker can use a forged token to bypass the issue ("iss") check during JSON web token	https://access.redhat.com/security/cve/CVE-2024-5037, https://bugzilla.redhat.com/show_bug.cgi?id=2272339, https://github.com/kubernetes	A-RED-OPEN-200624/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(JWT) authentication. **CVE ID: CVE-2024-5037**	/kubernetes/pull/123540	
Product: openshift_distributed_tracing					
Affected Version(s): 2.0					
Authentication Bypass by Spoofing	05-Jun-2024	7.5	A flaw was found in OpenShift's Telemeter. If certain conditions are in place, an attacker can use a forged token to bypass the issue ("iss") check during JSON web token (JWT) authentication. **CVE ID: CVE-2024-5037**	https://access.redhat.com/security/cve/CVE-2024-5037, https://bugzilla.redhat.com/show_bug.cgi?id=2272339, https://github.com/kubernetes/kubernetes/pull/123540	A-RED-OPEN-200624/499
Product: satellite					
Affected Version(s): 6.0					
N/A	05-Jun-2024	6.2	A flaw was found in foreman-installer when puppet-candlepin is invoked cpdb with the --password parameter. This issue leaks the password in the process list and allows an attacker to take advantage and obtain the password. **CVE ID: CVE-2024-3716**	N/A	A-RED-SATE-200624/500
Improper Neutralizat	05-Jun-2024	4.8	A flaw was found in the Katello plugin	N/A	A-RED-SATE-200624/501

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			for Foreman, where it is possible to store malicious JavaScript code in the "Description" field of a user. This code can be executed when opening certain pages, for example, Host Collections. **CVE ID: CVE-2024-4812**		
Vendor: reputeinfosystems					
Product: arforms					
Affected Version(s): * Up to (excluding) 6.4.1					
Missing Authorization	09-Jun-2024	8.8	Missing Authorization vulnerability in reputeinfosystems ARForms.This issue affects ARForms: from n/a through 6.4. **CVE ID: CVE-2024-32705**	N/A	A-REP-ARFO-200624/502
Vendor: risethemes					
Product: rt_easy_builder					
Affected Version(s): * Up to (excluding) 2.1					
Missing Authorization	04-Jun-2024	8.8	Missing Authorization vulnerability in RT Easy Builder – Advanced addons for Elementor.This issue affects RT Easy Builder – Advanced addons for Elementor:	N/A	A-RIS-RT_E-200624/503

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from n/a through 2.0. **CVE ID: CVE-2024-30484**		
Vendor: royal-elementor-addons					
Product: royal_elementor_addons					
Affected Version(s): * Up to (excluding) 1.3.977					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	5.4	The Royal Elementor Addons and Templates for WordPress is vulnerable to Stored Cross-Site Scripting via the 'inline_list' parameter in versions up to, and including, 1.3.976 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-4488**	https://plugins.trac.wordpress.org/changeset/3097775/	A-ROY-ROYA-200624/504
Improper Neutralization of Input During Web Page Generation	07-Jun-2024	5.4	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to	https://plugins.trac.wordpress.org/changeset/3097775/	A-ROY-ROYA-200624/505

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Stored Cross-Site Scripting via the 'custom_upload_mimes' function in versions up to, and including, 1.3.976 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-4489**		
Vendor: Rubyonrails					
Product: rails					
Affected Version(s): 7.2.0					
N/A	04-Jun-2024	9.8	Action Pack is a framework for handling and responding to web requests. Since 6.1.0, the application configurable Permissions-Policy is only served on responses with an HTML related Content-Type. This vulnerability is	https://github.com/rails/rails/commit/35858f1d9d57f6c4050a8d9ab754bd5d088b4523, https://github.com/rails/rails/security/advisories/GHSA-fwhr-88qx-h9g7	A-RUB-RAIL-200624/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in 6.1.7.8, 7.0.8.2, and 7.1.3.3. **CVE ID: CVE-2024-28103**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	6.1	Action Text brings rich text content and editing to Rails. Instances of ActionText::Attachable::ContentAttachment included within a rich_text_area tag could potentially contain unsanitized HTML. This vulnerability is fixed in 7.1.3.4 and 7.2.0.beta2. **CVE ID: CVE-2024-32464**	https://github.com/rails/rails/commit/e215bf3360e6dfe1497c1503a495e384ed6b0995	A-RUB-RAIL-200624/507
Affected Version(s): From (including) 6.1.0 Up to (excluding) 6.1.7.8					
N/A	04-Jun-2024	9.8	Action Pack is a framework for handling and responding to web requests. Since 6.1.0, the application configurable Permissions-Policy is only served on responses with an HTML related Content-Type. This vulnerability is fixed in 6.1.7.8, 7.0.8.2, and 7.1.3.3. **CVE ID: CVE-2024-28103**	https://github.com/rails/rails/commit/35858f1d9d57f6c4050a8d9ab754bd5d088b4523, https://github.com/rails/rails/security/advisories/GHSA-fwhr-88qx-h9g7	A-RUB-RAIL-200624/508
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.8.4					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jun-2024	9.8	Action Pack is a framework for handling and responding to web requests. Since 6.1.0, the application configurable Permissions-Policy is only served on responses with an HTML related Content-Type. This vulnerability is fixed in 6.1.7.8, 7.0.8.2, and 7.1.3.3. **CVE ID: CVE-2024-28103**	https://github.com/rails/rails/commit/35858f1d9d57f6c4050a8d9ab754bd5d088b4523, https://github.com/rails/rails/security/advisories/GHSA-fwhr-88qx-h9g7	A-RUB-RAIL-200624/509
Affected Version(s): From (including) 7.1.0 Up to (excluding) 7.1.3.4					
N/A	04-Jun-2024	9.8	Action Pack is a framework for handling and responding to web requests. Since 6.1.0, the application configurable Permissions-Policy is only served on responses with an HTML related Content-Type. This vulnerability is fixed in 6.1.7.8, 7.0.8.2, and 7.1.3.3. **CVE ID: CVE-2024-28103**	https://github.com/rails/rails/commit/35858f1d9d57f6c4050a8d9ab754bd5d088b4523, https://github.com/rails/rails/security/advisories/GHSA-fwhr-88qx-h9g7	A-RUB-RAIL-200624/510
Improper Neutralization of Input During Web Page	04-Jun-2024	6.1	Action Text brings rich text content and editing to Rails. Instances of ActionText::Attach	https://github.com/rails/rails/commit/e215bf3360e6dfe1497	A-RUB-RAIL-200624/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			able::ContentAttachment included within a rich_text_area tag could potentially contain unsanitized HTML. This vulnerability is fixed in 7.1.3.4 and 7.2.0.beta2. **CVE ID: CVE-2024-32464**	c1503a495e384ed6b0995	
Vendor: salesagility					
Product: suitecrm					
Affected Version(s): * Up to (excluding) 7.14.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	9.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in events response entry point allows for a SQL injection attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36412**	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-xjx2-38hv-5hh8	A-SAL-SUIT-200624/512
Improper Neutralization of Input During Web Page Generation	10-Jun-2024	9	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-3www-6rqc-rm7j	A-SAL-SUIT-200624/513

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			and 8.6.1, an unverified IFrame can be added some some inputs, which could allow for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36417**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in the `Alerts` controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36408**	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-2g8f-gjrr-x5cg	A-SAL-SUIT-200624/514
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-pxq4-vw23-v73f	A-SAL-SUIT-200624/515

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tree data entry point. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36409**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax messages count controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36410**	N/A	A-SAL-SUIT-200624/516
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax displayView controller. Versions 7.14.4 and 8.6.1	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-9rvr-mcrf-p4p7	A-SAL-SUIT-200624/517

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a fix for this issue. **CVE ID: CVE-2024-36411**		
Unrestricted Upload of File with Dangerous Type	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in uploaded file verification in products allows for remote code execution. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36415**	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-c82f-58jv-jfrh	A-SAL-SUIT-200624/518
N/A	10-Jun-2024	7.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a deprecated v4 API example with no log rotation allows denial of service by logging excessive data. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-jrpp-22g3-2j77	A-SAL-SUIT-200624/519

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36416		
Weak Password Recovery Mechanism for Forgotten Password	10-Jun-2024	6.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, a user password can be reset from an unauthenticated attacker. The attacker does not get access to the new password. But this can be annoying for the user. This attack is also dependent on some password reset functionalities being enabled. It also requires the system using php 7, which is not an officially supported version. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36407**	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-6p2f-wwx9-952r	A-SAL-SUIT-200624/520
Server-Side Request Forgery (SSRF)	10-Jun-2024	6.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-wg74-772c-8gr7	A-SAL-SUIT-200624/521

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to versions 7.14.4 and 8.6.1, a vulnerability in the connectors file verification allows for a server-side request forgery attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36414**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jun-2024	5.4	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in the import module error view allows for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36413**	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-ph2c-hvvf-r273	A-SAL-SUIT-200624/522
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.6.1					
Improper Neutralization of Special Elements used in an SQL Command	10-Jun-2024	9.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-xjx2-38hv-5hh8	A-SAL-SUIT-200624/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			vulnerability in events response entry point allows for a SQL injection attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36412**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jun-2024	9	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, an unverified IFrame can be added some some inputs, which could allow for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36417**	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-3www-6rqc-rm7j	A-SAL-SUIT-200624/524
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in the `Alerts`	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-2g8f-gjrr-x5cg	A-SAL-SUIT-200624/525

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36408**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in Tree data entry point. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36409**	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-pxq4-vw23-v73f	A-SAL-SUIT-200624/526
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax messages count controller. Versions 7.14.4 and 8.6.1	N/A	A-SAL-SUIT-200624/527

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a fix for this issue. **CVE ID: CVE-2024-36410**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax displayView controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36411**	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-9rvr-mcrf-p4p7	A-SAL-SUIT-200624/528
Unrestricted Upload of File with Dangerous Type	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in uploaded file verification in products allows for remote code execution. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-c82f-58jv-jfrh	A-SAL-SUIT-200624/529

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36415		
N/A	10-Jun-2024	7.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a deprecated v4 API example with no log rotation allows denial of service by logging excessive data. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36416**	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-jrpp-22g3-2j77	A-SAL-SUIT-200624/530
Weak Password Recovery Mechanism for Forgotten Password	10-Jun-2024	6.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, a user password can be reset from an unauthenticated attacker. The attacker does not get access to the new password. But this can be annoying for the user. This attack is also dependent on some password	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-6p2f-wwx9-952r	A-SAL-SUIT-200624/531

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset functionalities being enabled. It also requires the system using php 7, which is not an officially supported version. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36407**		
Server-Side Request Forgery (SSRF)	10-Jun-2024	6.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in the connectors file verification allows for a server-side request forgery attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36414**	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-wg74-772c-8gr7	A-SAL-SUIT-200624/532
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jun-2024	5.4	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in the	https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-ph2c-hvvf-r273	A-SAL-SUIT-200624/533

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			import module error view allows for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. **CVE ID: CVE-2024-36413**		
Vendor: sc_filechecker_project					
Product: sc_filechecker					
Affected Version(s): * Up to (including) 0.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	6.5	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Siteclean SC filechecker allows Path Traversal, File Manipulation.This issue affects SC filechecker: from n/a through 0.6. **CVE ID: CVE-2024-35743**	N/A	A-SC_-SC_F-200624/534
Vendor: seacms					
Product: seacms					
Affected Version(s): 12.9					
N/A	10-Jun-2024	9.1	SeaCMS 12.9 has a file deletion vulnerability via admin_template.php. **CVE ID: CVE-2024-31611**	N/A	A-SEA-SEAC-200624/535
Vendor: securenvoy					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: multi-factor_authentication_solutions					
Affected Version(s): * Up to (excluding) 9.4.514					
Cleartext Transmission of Sensitive Information	10-Jun-2024	7.5	Multiple LDAP injections vulnerabilities exist in SecurEnvoy MFA before 9.4.514 due to improper validation of user-supplied input. An unauthenticated remote attacker could exfiltrate data from Active Directory through blind LDAP injection attacks against the DESKTOP service exposed on the /secserver HTTP endpoint. This may include ms-Mcs-AdmPwd, which has a cleartext password for the Local Administrator Password Solution (LAPS) feature. **CVE ID: CVE-2024-37393**	N/A	A-SEC-MULT-200624/536
Vendor: seedprod					
Product: rafflepress					
Affected Version(s): * Up to (excluding) 1.12.5					
Missing Authorization	10-Jun-2024	6.3	Missing Authorization vulnerability in RafflePress Giveaways and Contests by RafflePress.This	N/A	A-SEE-RAFF-200624/537

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects Giveaways and Contests by RafflePress: from n/a through 1.12.4. **CVE ID: CVE-2024-4745**		
Vendor: select-themes					
Product: stockholm					
Affected Version(s): * Up to (excluding) 9.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jun-2024	9.8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm allows PHP Local File Inclusion.This issue affects Stockholm: from n/a through 9.6. **CVE ID: CVE-2024-34551**	N/A	A-SEL-STOC-200624/538
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jun-2024	8.8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm allows PHP Local File Inclusion.This issue affects Stockholm: from n/a through 9.6.	N/A	A-SEL-STOC-200624/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-34552		
Product: stockholm_core					
Affected Version(s): * Up to (excluding) 2.4.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jun-2024	8.8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm Core allows PHP Local File Inclusion.This issue affects Stockholm Core: from n/a through 2.4.1. **CVE ID: CVE-2024-34554**	N/A	A-SEL-STOC-200624/540
Vendor: sendinblue					
Product: newsletter\,_smtp\,_email_marketing_and_subscribe					
Affected Version(s): * Up to (excluding) 3.1.78					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brevo Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue allows Reflected XSS.This issue affects Newsletter, SMTP, Email marketing and Subscribe	N/A	A-SEN-NEWS-200624/541

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			forms by Sendinblue: from n/a through 3.1.77. **CVE ID: CVE-2024-35668**		
Vendor: sinaextra					
Product: sina_extension_for_elementor					
Affected Version(s): * Up to (excluding) 3.5.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jun-2024	8.8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in SinaExtra Sina Extension for Elementor allows PHP Local File Inclusion.This issue affects Sina Extension for Elementor: from n/a through 3.5.1. **CVE ID: CVE-2024-34384**	N/A	A-SIN-SINA-200624/542
Vendor: softlabbd					
Product: integrate_google_drive					
Affected Version(s): * Up to (excluding) 1.3.94					
Improper Authentication	04-Jun-2024	9.8	Broken Authentication vulnerability in SoftLab Integrate Google Drive.This issue affects Integrate Google Drive: from n/a through 1.3.93. **CVE ID: CVE-2024-35670**	N/A	A-SOF-INTE-200624/543

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: upload_fields_for_wpforms					
Affected Version(s): * Up to (including) 1.0.2					
Missing Authorization	09-Jun-2024	9.8	Missing Authorization vulnerability in SoftLab Upload Fields for WPForms.This issue affects Upload Fields for WPForms: from n/a through 1.0.2. **CVE ID: CVE-2024-35661**	N/A	A-SOF-UPLO-200624/544
Vendor: Solarwinds					
Product: serv-u					
Affected Version(s): * Up to (excluding) 15.4.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jun-2024	7.5	SolarWinds Serv-U was susceptible to a directory transversal vulnerability that would allow access to read sensitive	https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28995	A-SOL-SERV-200624/545

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files on the host machine. **CVE ID: CVE-2024-28995**		
Affected Version(s): 15.4.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jun-2024	7.5	SolarWinds Serv-U was susceptible to a directory transversal vulnerability that would allow access to read sensitive files on the host machine. **CVE ID: CVE-2024-28995**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28995	A-SOL-SERV-200624/546
Product: solarwinds_platform					
Affected Version(s): * Up to (excluding) 2024.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jun-2024	8.1	The SolarWinds Platform was determined to be affected by a SWQL Injection Vulnerability. Attack complexity is high for this vulnerability. **CVE ID: CVE-2024-28996**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28996	A-SOL-SOLA-200624/547
Concurrent Execution using Shared	04-Jun-2024	8.1	The SolarWinds Platform was determined to be affected by a Race	https://www.solarwinds.com/trust-center/security-	A-SOL-SOLA-200624/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Condition Vulnerability affecting the web console. **CVE ID: CVE-2024-28999**	advisories/CVE-2024-28999	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	4.8	The SolarWinds Platform was determined to be affected by a stored cross-site scripting vulnerability affecting the web console. A high-privileged user and user interaction is required to exploit this vulnerability. **CVE ID: CVE-2024-29004**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-29004	A-SOL-SOLA-200624/549
Vendor: spiffyplugins					
Product: spiffy_calendar					
Affected Version(s): * Up to (excluding) 4.9.11					
Missing Authorization	04-Jun-2024	6.3	Missing Authorization vulnerability in Spiffy Plugins Spiffy Calendar.This issue affects Spiffy Calendar: from n/a through 4.9.10. **CVE ID: CVE-2024-30528**	N/A	A-SPI-SPIF-200624/550
Product: wp_flow_plus					
Affected Version(s): * Up to (excluding) 5.2.3					
Improper Neutralization of Input During	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation	N/A	A-SPI-WP_F-200624/551

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			(XSS or 'Cross-site Scripting') vulnerability in Spiffy Plugins WP Flow Plus allows Stored XSS.This issue affects WP Flow Plus: from n/a through 5.2.2. **CVE ID: CVE-2024-35651**		
Vendor: stock_management_system_project					
Product: stock_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jun-2024	9.8	Sourcecodester Stock Management System v1.0 is vulnerable to SQL Injection via editCategories.php. **CVE ID: CVE-2024-36779**	N/A	A-STO-STOC-200624/552
Vendor: strategery-migrations_project					
Product: strategery-migrations					
Affected Version(s): * Up to (including) 1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	7.5	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Gabriel Somoza / Joseph Fitzgibbons Strategery Migrations allows Path Traversal, File Manipulation.This issue affects	N/A	A-STR-STRA-200624/553

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Strategery Migrations: from n/a through 1.0. **CVE ID: CVE-2024-35745**		
Vendor: stylemixthemes					
Product: mega_menu					
Affected Version(s): * Up to (excluding) 2.3.13					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	9.8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in StylemixThemes MegaMenu allows PHP Local File Inclusion.This issue affects MegaMenu: from n/a through 2.3.12. **CVE ID: CVE-2024-35677**	N/A	A-STY-MEGA-200624/554
Vendor: summar					
Product: mentor					
Affected Version(s): 3.83.35					
Deserialization of Untrusted Data	06-Jun-2024	9.8	Untrusted data deserialization vulnerability has been found in Mentor - Employee Portal, affecting version 3.83.35. This vulnerability could allow an attacker to execute arbitrary code, by injecting a malicious payload	N/A	A-SUM-MENT-200624/555

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into the "ViewState" field. **CVE ID: CVE-2024-5675**		
Vendor: Sysaid					
Product: sysaid					
Affected Version(s): * Up to (including) 23.3.38					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jun-2024	9.8	SysAid - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') **CVE ID: CVE-2024-36393**	N/A	A-SYS-SYSA-200624/556
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Jun-2024	9.8	SysAid - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') **CVE ID: CVE-2024-36394**	N/A	A-SYS-SYSA-200624/557
Vendor: themehigh					
Product: checkout_field_editor_for_woocommerce					
Affected Version(s): * Up to (excluding) 3.6.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	9.1	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ThemeHigh Checkout Field	N/A	A-THE-CHEC-200624/558

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Editor for WooCommerce (Pro) allows Functionality Misuse, File Manipulation.This issue affects Checkout Field Editor for WooCommerce (Pro): from n/a through 3.6.2. **CVE ID: CVE-2024-35658**		
Vendor: themeisle					
Product: product_addons_\&_fields_for_woocommerce					
Affected Version(s): * Up to (excluding) 32.0.21					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-Jun-2024	5.3	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Themeisle PPOM for WooCommerce allows Code Inclusion.This issue affects PPOM for WooCommerce: from n/a through 32.0.20. **CVE ID: CVE-2024-35728**	N/A	A-THE-PROD-200624/559
Vendor: themekraft					
Product: buddyforms					
Affected Version(s): * Up to (including) 2.8.9					
Use of Insufficient	05-Jun-2024	5.3	The BuddyForms plugin for	N/A	A-THE-BUDD-200624/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			WordPress is vulnerable to Email Verification Bypass in all versions up to, and including, 2.8.9 via the use of an insufficiently random activation code. This makes it possible for unauthenticated attackers to bypass the email verification. **CVE ID: CVE-2024-5149**		
Product: buddypress_woocommerce_my_account_integration._create_woocommerce_member_pages					
Affected Version(s): * Up to (excluding) 3.4.20					
Missing Authorization	10-Jun-2024	8.8	Missing Authorization vulnerability in ThemeKraft WooBuddy.This issue affects WooBuddy: from n/a through 3.4.19. **CVE ID: CVE-2024-35726**	N/A	A-THE-BUDD-200624/561
Vendor: themesflat					
Product: themesflat_addons_for_elementor					
Affected Version(s): * Up to (including) 2.1.2					
Improper Neutralization of Input During Web Page Generation	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themesflat	N/A	A-THE-THEM-200624/562

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Themesflat Addons For Elementor allows Stored XSS.This issue affects Themesflat Addons For Elementor: from n/a through 2.1.2. **CVE ID: CVE-2024-35666**		
Vendor: themeum					
Product: tutor_lms					
Affected Version(s): * Up to (excluding) 2.7.2					
Authorization Bypass Through User-Controlled Key	07-Jun-2024	4.3	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.7.1 via the 'attempt_delete' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Instructor-level access and above, to delete arbitrary quiz attempts. **CVE ID: CVE-2024-5438**	https://plugins.trac.wordpress.org/changeset/3098465/	A-THE-TUTO-200624/563
Vendor: thenewsletterplugin					
Product: newsletter					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 8.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	6.1	The Newsletter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'np1' parameter in all versions up to, and including, 8.3.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5317**	https://plugins.trac.wordpress.org/changeset/3095002/newsletter	A-THE-NEWS-200624/564
Vendor: thimpress					
Product: learnpress					
Affected Version(s): * Up to (excluding) 4.2.6.8.1					
N/A	05-Jun-2024	5.3	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.2.6.8 due to incorrect implementation of get_items_permissi	N/A	A-THI-LEAR-200624/565

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ons_check function. This makes it possible for unauthenticated attackers to extract basic information about website users, including their emails **CVE ID: CVE-2024-5483**		
Vendor: tickera					
Product: tickera					
Affected Version(s): * Up to (excluding) 3.5.2.7					
Missing Authorization	10-Jun-2024	8.8	Missing Authorization vulnerability in Tickera.This issue affects Tickera: from n/a through 3.5.2.6. **CVE ID: CVE-2024-35729**	N/A	A-TIC-TICK-200624/566
Vendor: tnbmobil					
Product: cockpit					
Affected Version(s): * Up to (excluding) 0.251.1					
N/A	05-Jun-2024	7.5	Inclusion of Sensitive Information in Source Code vulnerability in TNB Mobile Solutions Cockpit Software allows Retrieve Embedded Sensitive Data.This issue affects Cockpit Software: before v0.251.1.	N/A	A-TNB-COCK-200624/567

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-1272		
Vendor: tribe29					
Product: checkmk					
Affected Version(s): 2.3.0					
Improper Restriction of Excessive Authentication Attempts	10-Jun-2024	7.5	Improper restriction of excessive authentication attempts with two factor authentication methods in Checkmk 2.3 before 2.3.0p6 facilitates brute-forcing of second factor mechanisms. **CVE ID: CVE-2024-28833**	https://checkmk.com/werk/16830	A-TRI-CHEC-200624/568
Vendor: unlimited-elements					
Product: unlimited_elements_for_elementor_\(free_widgets\,_addons\,_templates\)					
Affected Version(s): * Up to (excluding) 1.5.110					
Missing Authorization	05-Jun-2024	8.8	Missing Authorization vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates).This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from	N/A	A-UNL-UNLI-200624/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			n/a through 1.5.109. **CVE ID: CVE-2024-35674**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jun-2024	8.8	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to blind SQL Injection via the 'data[addonID]' parameter in all versions up to, and including, 1.5.109 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-5329**	https://plugins.trac.wordpress.org/changeset/3097249/#file6	A-UNL-UNLI-200624/570
Vendor: upunzipper_project					
Product: upunzipper					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	6.5	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ravidhu Dissanayake Upunzipper allows Path Traversal, File Manipulation.This issue affects Upunzipper: from n/a through 1.0.0. **CVE ID: CVE-2024-35744**	N/A	A-UPU-UPUN-200624/571
Vendor: userproplugin					
Product: userpro					
Affected Version(s): * Up to (excluding) 5.1.9					
N/A	04-Jun-2024	9.8	Improper Privilege Management vulnerability in DeluxeThemes Userpro allows Privilege Escalation.This issue affects Userpro: from n/a through 5.1.8. **CVE ID: CVE-2024-35700**	N/A	A-USE-USER-200624/572
Vendor: vanyukov					
Product: market_exporter					
Affected Version(s): * Up to (excluding) 2.0.20					
Improper Limitation of a Pathname	07-Jun-2024	8.1	The Market Exporter plugin for WordPress is vulnerable to	https://plugins.trac.wordpress.org/changeset/3098360/mark	A-VAN-MARK-200624/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			unauthorized loss of data due to a missing capability check on the 'remove_files' function in all versions up to, and including, 2.0.19. This makes it possible for authenticated attackers, with Subscriber-level access and above, to use path traversal to delete arbitrary files on the server. **CVE ID: CVE-2024-5637**	et-exporter/trunk/includes/class-restapi.php	
Vendor: Videowhisper					
Product: picture_gallery					
Affected Version(s): * Up to (excluding) 1.5.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in VideoWhisper Picture Gallery allows Stored XSS.This issue affects Picture Gallery: from n/a through 1.5.11. **CVE ID: CVE-2024-34759**	N/A	A-VID-PICT-200624/574
Vendor: visualcomposer					
Product: visual_composer_website_builder					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 45.9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in visualcomposer.Com Visual Composer Website Builder allows Stored XSS.This issue affects Visual Composer Website Builder: from n/a through 45.8.0. **CVE ID: CVE-2024-35653**	N/A	A-VIS-VISU-200624/575
Vendor: viz					
Product: nano_id					
Affected Version(s): * Up to (excluding) 0.4.0					
Insufficient Entropy	04-Jun-2024	9.8	nano-id is a unique string ID generator for Rust. Affected versions of the nano-id crate incorrectly generated IDs using a reduced character set in the `nano_id::base62` and `nano_id::base58` functions. Specifically, the `base62` function used a character set of 32 symbols instead of the intended 62 symbols, and the	https://github.com/viz-rs/nano-id/commit/a9022772b2f1ce38929b5b81eccc670ac9d3ab23, https://github.com/viz-rs/nano-id/security/advisories/GHSA-9hc7-6w9r-wj94	A-VIZ-NANO-200624/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`base58` function used a character set of 16 symbols instead of the intended 58 symbols. Additionally, the `nano_id::gen` macro is also affected when a custom character set that is not a power of 2 in size is specified. It should be noted that `nano_id::base64` is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. **CVE ID: CVE-2024-36400**		
Vendor: vollstart					
Product: event_tickets_with_ticket_scanner					
Affected Version(s): * Up to (excluding) 2.3.2					
Improper Neutralization of Input	04-Jun-2024	6.1	Improper Neutralization of Input During Web	N/A	A-VOL-EVEN-200624/577

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Page Generation (XSS or 'Cross-site Scripting') vulnerability in Saso Nikolov Event Tickets with Ticket Scanner allows Reflected XSS.This issue affects Event Tickets with Ticket Scanner: from n/a through 2.3.1. **CVE ID: CVE-2024-35652**		
Vendor: wbcomdesigns					
Product: custom_font_uploader					
Affected Version(s): * Up to (excluding) 2.4.0					
Missing Authorization	06-Jun-2024	4.3	The Wbcom Designs – Custom Font Uploader plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'cfu_delete_customfont' function in all versions up to, and including, 2.3.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete any custom font. **CVE ID: CVE-2024-5489**	https://plugins.trac.wordpress.org/changeset/3097373/	A-WBC-CUST-200624/578

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: weavertheme					
Product: weaver_xtreme_theme_support					
Affected Version(s): * Up to (excluding) 6.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Weaver Xtreme Theme Support plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's div shortcode in all versions up to, and including, 6.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-4939**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3095286%40weaverx-theme-support%2Ftrunk&old=3017943%40weaverx-theme-support%2Ftrunk&sfp_email=&sfph_mail=	A-WEA-WEAV-200624/579
Vendor: web-audimex					
Product: audimexee					
Affected Version(s): 15.1.2					
Improper Neutralization of Input During Web Page Generation	04-Jun-2024	5.4	Cross Site Scripting vulnerability in audimex audimexEE v.15.1.2 and fixed in 15.1.3.9 allows a	N/A	A-WEB-AUDI-200624/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			remote attacker to execute arbitrary code via the service, method, widget_type, request_id, payload parameters. **CVE ID: CVE-2024-30889**		
Vendor: websupporter_filter_custom_fields_\&_taxonomies_light_project					
Product: websupporter_filter_custom_fields_\&_taxonomies_light					
Affected Version(s): * Up to (including) 1.05					
Missing Authorization	09-Jun-2024	8.8	Missing Authorization vulnerability in Websupporter Filter Custom Fields & Taxonomies Light.This issue affects Filter Custom Fields & Taxonomies Light: from n/a through 1.05. **CVE ID: CVE-2024-32081**	N/A	A-WEB-WEBS-200624/581
Vendor: westguardsolutions					
Product: ws_form					
Affected Version(s): * Up to (excluding) 1.9.218					
Improper Neutralization of Formula Elements in a CSV File	07-Jun-2024	8.8	The WS Form LITE plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 1.9.217. This allows unauthenticated attackers to embed	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3098265%40ws-form&new=3098265%40ws-	A-WES-WS_F-200624/582

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			untrusted input into exported CSV files, which can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration. **CVE ID: CVE-2023-5424**	form&sfp_email=&sfph_mail=	
Vendor: willnorris					
Product: open_graph					
Affected Version(s): * Up to (excluding) 1.11.3					
N/A	06-Jun-2024	5.3	The Open Graph plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.11.2 via the 'opengraph_default_description' function. This makes it possible for unauthenticated attackers to extract sensitive data including partial content of password-protected blog posts. **CVE ID: CVE-2024-5615**	https://plugins.trac.wordpress.org/changeset/3097574/	A-WIL-OPEN-200624/583

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wobbie					
Product: mollie_forms					
Affected Version(s): * Up to (excluding) 2.6.14					
Cross-Site Request Forgery (CSRF)	05-Jun-2024	4.3	The Mollie Forms plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.13. This is due to missing or incorrect nonce validation on the duplicateForm() function. This makes it possible for unauthenticated attackers to duplicate forms via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-2368**	https://plugins.trac.wordpress.org/changeset/3097426/mollie-forms	A-WOB-MOLL-200624/584
Vendor: woostify					
Product: boostify_header_footer_builder_for_elementor					
Affected Version(s): * Up to (excluding) 1.3.3					
Improper Neutralization of Input During Web Page Generation	05-Jun-2024	5.4	The Boostify Header Footer Builder for Elementor plugin for WordPress is vulnerable to Stored Cross-Site	https://plugins.trac.wordpress.org/changeset/3097085/#file9	A-WOO-BOOS-200624/585

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting via the 'size' parameter in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5006**		
Vendor: wow-company					
Product: easy_digital_downloads					
Affected Version(s): * Up to (including) 1.0.2					
Inclusion of Functionality from Untrusted Control Sphere	04-Jun-2024	9.8	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Wow-Company Easy Digital Downloads – Recent Purchases allows PHP Remote File Inclusion.This issue affects Easy Digital Downloads – Recent Purchases:	N/A	A-WOW-EASY-200624/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from n/a through 1.0.2. **CVE ID: CVE-2024-35629**		
Product: woocommerce_-_recent_purchases					
Affected Version(s): * Up to (including) 1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jun-2024	4.9	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Wow-Company Woocommerce – Recent Purchases allows PHP Local File Inclusion.This issue affects Woocommerce – Recent Purchases: from n/a through 1.0.1. **CVE ID: CVE-2024-35634**	N/A	A-WOW-WOOC-200624/587
Vendor: wpattire					
Product: attire_blocks					
Affected Version(s): * Up to (excluding) 1.9.3					
Missing Authorization	05-Jun-2024	4.3	The Gutenberg Blocks and Page Layouts – Attire Blocks plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the disable_fe_assets function in all	https://plugins.trac.wordpress.org/changeset/3085600/attire-blocks/trunk/admin/AttireBlocksSettings.php?old=2996841&old_path=attire-blocks%2Ftrunk%2Fadmin%2	A-WPA-ATTI-200624/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions up to, and including, 1.9.2. This makes it possible for authenticated attackers, with subscriber access or above, to change the plugin's settings. Additionally, no nonce check is performed resulting in a CSRF vulnerability. **CVE ID: CVE-2024-4088**	FAttireBlocksSettings.php	
Vendor: wpdeveloper					
Product: embedpress					
Affected Version(s): * Up to (excluding) 3.9.9					
Missing Authorization	09-Jun-2024	9.8	Missing Authorization vulnerability in WPDeveloper EmbedPress.This issue affects EmbedPress: from n/a through 3.9.8. **CVE ID: CVE-2024-31284**	N/A	A-WPD-EMBE-200624/589
Affected Version(s): * Up to (excluding) 4.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The EmbedPress – Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor plugin	https://plugins.trac.wordpress.org/changeset/3097114/	A-WPD-EMBE-200624/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' attribute within the plugin's EmbedPress PDF widget in all versions up to, and including, 4.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5571**		
Product: essential_addons_for_elementor					
Affected Version(s): * Up to (excluding) 5.9.23					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-2024	5.4	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'get_manual_calend	https://plugins.trac.wordpress.org/changeset/3097900/	A-WPD-ESSE-200624/591

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ar_events' function in all versions up to, and including, 5.9.22 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5188**		
Vendor: wpdownloadmanager					
Product: download_manager					
Affected Version(s): * Up to (excluding) 3.2.94					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpdm_modal_login_form' shortcode in all versions up to, and including, 3.2.93 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible	https://plugins.trac.wordpress.org/changeset/3096459/	A-WPD-DOWN-200624/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-4001**		
Vendor: wpfactory					
Product: products\,_order_\&_customers_export_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.0.9					
Missing Authorization	09-Jun-2024	9.8	Missing Authorization vulnerability in WPFactory Products, Order & Customers Export for WooCommerce.This issue affects Products, Order & Customers Export for WooCommerce: from n/a through 2.0.8. **CVE ID: CVE-2024-31276**	N/A	A-WPF-PROD-200624/593
Vendor: wpfoxly					
Product: adfoxly					
Affected Version(s): * Up to (including) 1.8.5					
Missing Authorization	09-Jun-2024	9.8	Missing Authorization vulnerability in AdFoxly AdFoxly – Ad Manager, AdSense Ads &	N/A	A-WPF-ADFO-200624/594

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ads.Txt.This issue affects AdFoxly – Ad Manager, AdSense Ads & Ads.Txt: from n/a through 1.8.5. **CVE ID: CVE-2024-34802**		
Vendor: wpvivid					
Product: wpvivid_backup_for_mainwp					
Affected Version(s): * Up to (excluding) 0.9.33					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPvivid Team WPvivid Backup for MainWP allows Reflected XSS.This issue affects WPvivid Backup for MainWP: from n/a through 0.9.32. **CVE ID: CVE-2024-35664**	N/A	A-WPV-WPVI-200624/595
Vendor: xootix					
Product: login\/signup_popup					
Affected Version(s): From (including) 2.7.1 Up to (excluding) 2.7.3					
Missing Authorization	06-Jun-2024	4.3	The Login/Signup Popup (Inline Form + Woocommerce) plugin for WordPress is vulnerable to unauthorized access of data due	https://plugins.trac.wordpress.org/changeset/3093994/	A-XOO-LOGI-200624/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a missing capability check on the 'export_settings' function in versions 2.7.1 to 2.7.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read arbitrary options on affected sites. **CVE ID: CVE-2024-5665**		
Vendor: yithemes					
Product: yith_woocommerce_product_add-ons					
Affected Version(s): * Up to (excluding) 4.9.3					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-Jun-2024	5.3	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in YITH YITH WooCommerce Product Add-Ons allows Code Injection.This issue affects YITH WooCommerce Product Add-Ons: from n/a through 4.9.2. **CVE ID: CVE-2024-35680**	N/A	A-YIT-YITH-200624/597
Vendor: zorem					
Product: advanced_local_pickup_for_woocommerce					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.6.3					
Missing Authorization	09-Jun-2024	9.8	Missing Authorization vulnerability in zorem Advanced Local Pickup for WooCommerce.This issue affects Advanced Local Pickup for WooCommerce: from n/a through 1.6.2. **CVE ID: CVE-2024-31283**	N/A	A-ZOR-ADVA-200624/598
Hardware					
Vendor: ABB					
Product: 2tma310010b0001					
Affected Version(s): -					
Exposure of Sensitive Information to an Unauthorized Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System **CVE ID: CVE-2024-4008**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-2TMA-200624/599
Authentication Bypass by Capture-replay	05-Jun-2024	7.8	Replay Attack in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-2TMA-200624/600

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local KNX Bus-System **CVE ID: CVE-2024-4009**		
Product: 2tma310010b0003					
Affected Version(s): -					
Exposure of Sensitive Information to an Unauthorized Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System **CVE ID: CVE-2024-4008**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-2TMA-200624/601
Authentication Bypass by Capture-replay	05-Jun-2024	7.8	Replay Attack in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System **CVE ID: CVE-2024-4009**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-2TMA-200624/602
Product: 2tma310011b0001					
Affected Version(s): -					
Exposure of Sensitive Information to an Unauthorized Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&Docume	H-ABB-2TMA-200624/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to local KNX Bus-System **CVE ID: CVE-2024-4008**	ntPartId=&Action=Launch	
Authentication Bypass by Capture-replay	05-Jun-2024	7.8	Replay Attack in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System **CVE ID: CVE-2024-4009**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-2TMA-200624/604
Product: 2tma310011b0002					
Affected Version(s): -					
Exposure of Sensitive Information to an Unauthorized Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System **CVE ID: CVE-2024-4008**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-2TMA-200624/605
Authentication Bypass by Capture-replay	05-Jun-2024	7.8	Replay Attack in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-2TMA-200624/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KNX telegram to local KNX Bus-System **CVE ID: CVE-2024-4009**		
Product: 2tma310011b0003					
Affected Version(s): -					
Exposure of Sensitive Information to an Unauthorized Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System **CVE ID: CVE-2024-4008**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-2TMA-200624/607
Authentication Bypass by Capture-replay	05-Jun-2024	7.8	Replay Attack in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System **CVE ID: CVE-2024-4009**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-2TMA-200624/608
Vendor: Mitel					
Product: 6869i_sip					
Affected Version(s): -					
Improper Neutralization of Special	09-Jun-2024	8.8	An issue was discovered on Mitel 6869i through 4.5.0.41 and 5.x	N/A	H-MIT-6869-200624/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			through 5.0.0.1018 devices. A command injection vulnerability exists in the hostname parameter taken in by the provis.html endpoint. The provis.html endpoint performs no sanitization on the hostname parameter (sent by an authenticated user), which is subsequently written to disk. During boot, the hostname parameter is executed as part of a series of shell commands. Attackers can achieve remote code execution in the root context by placing shell metacharacters in the hostname parameter. **CVE ID: CVE-2024-37569**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Jun-2024	8.8	On Mitel 6869i 4.5.0.41 devices, the Manual Firmware Update (upgrade.html) page does not perform sanitization on the username and path parameters (sent	N/A	H-MIT-6869-200624/610

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by an authenticated user) before appending flags to the busybox ftpget command. This leads to $() command execution. **CVE ID: CVE-2024-37570**		
Vendor: Samsung					
Product: exynos_1080					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/611

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/612
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/613

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/614
Product: exynos_1280					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor,	https://semiconductor.samsung.com/support/quality-	H-SAM-EXYN-200624/615

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	support/product-security-updates/	
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/617
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and	https://semiconductor.samsung.com/support/quality-support/produc	H-SAM-EXYN-200624/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	t-security-updates/	
Product: exynos_1330					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/619

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/620
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/621

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/622

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: exynos_1380					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/623
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/624

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/625

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/626
Product: exynos_2100					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/628
Missing Encryption	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile	https://semiconductor.samsung.com/support/q	H-SAM-EXYN-200624/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	uality-support/product-security-updates/	
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/630

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**		
Product: exynos_2200					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/631
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor,	https://semiconductor.samsung.com/support/quality-support/produc	H-SAM-EXYN-200624/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	t-security-updates/	
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/634
Product: exynos_2400					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/635

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
Product: exynos_850					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control)	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/636

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/637
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/638

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/639

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: exynos_9110					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/640
Product: exynos_980					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to disclosure of sensitive information. **CVE ID: CVE-2023-49928**		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/643
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/644

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**		
Product: exynos_9820					
Affected Version(s): -					
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-49928		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/646
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/647

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**		
Product: exynos_9825					
Affected Version(s): -					
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/648
Missing Encryption	05-Jun-2024	5.3	An issue was discovered in	https://semiconductor.samsung	H-SAM-EXYN-200624/649

CVSSv3 Scoring Scale: 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	.com/support/quality-support/product-security-updates/	
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**		
Product: exynos_990					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/651
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive	https://semiconductor.samsung.com/support/quality-support/produc	H-SAM-EXYN-200624/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	t-security-updates/	
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/653

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/654
Product: exynos_auto_t5123					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
Product: exynos_modem_5123					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/656

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/657
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable	https://semiconductor.samsung.com/support/quality-support/produc	H-SAM-EXYN-200624/658

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	t-security-updates/	
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/659

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-50803		
Product: exynos_modem_5300					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/660
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/662

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/663
Product: exynos_w920					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/664

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
Product: exynos_w930					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200624/665

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
Vendor: Tendacn					
Product: o3v2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Jun-2024	9.8	Tenda O3V2 v1.0.0.12(3880) was discovered to contain a Blind Command Injection via stpEn parameter in the SetStp function. This vulnerability allows attackers to execute arbitrary commands with root privileges. **CVE ID: CVE-2024-36604**	N/A	H-TEN-O3V2-200624/666
Vendor: uniview					
Product: nvr301-04s2-p4					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jun-2024	5.4	Uniview NVR301-04S2-P4 is vulnerable to reflected cross-site scripting attack (XSS). An attacker could send a user a URL that if clicked on could execute malicious JavaScript in their browser. This vulnerability also requires	N/A	H-UNI-NVR3-200624/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication before it can be exploited, so the scope and severity is limited. Also, even if JavaScript is executed, no additional benefits are obtained. **CVE ID: CVE-2024-3850**		
Vendor: vw					
Product: id.charger_connect					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass	N/A	H-VW-ID.C-200624/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism. **CVE ID: CVE-2024-5684**		
Product: id.charger_pro					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated	N/A	H-VW-ID.C-200624/669

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can exploit this vulnerability to bypass the authentication mechanism. **CVE ID: CVE-2024-5684**		
Operating System					
Vendor: ABB					
Product: 2tma310010b0001_firmware					
Affected Version(s): * Up to (excluding) 1.02					
Exposure of Sensitive Information to an Unauthorized Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System **CVE ID: CVE-2024-4008**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-2TMA-200624/670
Authentication Bypass by Capture-replay	05-Jun-2024	7.8	Replay Attack in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System **CVE ID: CVE-2024-4009**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-2TMA-200624/671
Product: 2tma310010b0003_firmware					
Affected Version(s): * Up to (excluding) 1.02					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System **CVE ID: CVE-2024-4008**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A08803&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-2TMA-200624/672
Authentication Bypass by Capture-replay	05-Jun-2024	7.8	Replay Attack in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System **CVE ID: CVE-2024-4009**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A08803&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-2TMA-200624/673
Product: 2tma310011b0001_firmware					
Affected Version(s): * Up to (excluding) 1.02					
Exposure of Sensitive Information to an Unauthorized Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System **CVE ID: CVE-2024-4008**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A08803&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-2TMA-200624/674
Authentication Bypass by	05-Jun-2024	7.8	Replay Attack	https://search.abb.com/library/Download.aspx?	O-ABB-2TMA-200624/675

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System **CVE ID: CVE-2024-4009**	DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	
Product: 2tma310011b0002_firmware					
Affected Version(s): * Up to (excluding) 1.02					
Exposure of Sensitive Information to an Unauthorized Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System **CVE ID: CVE-2024-4008**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-2TMA-200624/676
Authentication Bypass by Capture-replay	05-Jun-2024	7.8	Replay Attack in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System **CVE ID: CVE-2024-4009**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-2TMA-200624/677
Product: 2tma310011b0003_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.02					
Exposure of Sensitive Information to an Unauthorized Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System **CVE ID: CVE-2024-4008**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A08803&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-2TMA-200624/678
Authentication Bypass by Capture-replay	05-Jun-2024	7.8	Replay Attack in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System **CVE ID: CVE-2024-4009**	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A08803&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-2TMA-200624/679
Vendor: Apple					
Product: macos					
Affected Version(s): * Up to (excluding) 12.5					
Out-of-bounds Write	10-Jun-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Monterey 12.5. Processing a maliciously crafted tiff file may lead to	https://support.apple.com/en-us/HT213345	O-APP-MACO-200624/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID: CVE-2022-32897**		
Out-of-bounds Read	10-Jun-2024	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.5. Processing an AppleScript may result in unexpected termination or disclosure of process memory. **CVE ID: CVE-2022-48578**	https://support.apple.com/en-us/HT213345	O-APP-MACO-200624/681
N/A	10-Jun-2024	5.3	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Monterey 12.5. A website may be able to track the websites a user visited in Safari private browsing mode. **CVE ID: CVE-2022-32933**	https://support.apple.com/en-us/HT213345	O-APP-MACO-200624/682
Affected Version(s): * Up to (excluding) 12.7.4					
N/A	10-Jun-2024	8.6	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Ventura 13.6.5,	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support	O-APP-MACO-200624/683

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.7.4. An app may be able to break out of its sandbox. **CVE ID: CVE-2024-23299**	.apple.com/en-us/HT214085	
N/A	10-Jun-2024	5.5	The issue was addressed with improved restriction of data container access. This issue is fixed in macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to access sensitive user data. **CVE ID: CVE-2023-40389**	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214085	O-APP-MACO-200624/684
Affected Version(s): * Up to (excluding) 13.0					
N/A	10-Jun-2024	7.8	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13. An app may be able to break out of its sandbox. **CVE ID: CVE-2022-48683**	https://support.apple.com/en-us/HT213488	O-APP-MACO-200624/685
Affected Version(s): * Up to (excluding) 14.4					
N/A	10-Jun-2024	5.5	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Sonoma 14.4. An app may be	https://support.apple.com/en-us/HT214084	O-APP-MACO-200624/686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to access user-sensitive data. **CVE ID: CVE-2024-27792**		
Affected Version(s): From (including) 13.0 Up to (excluding) 13.6.5					
N/A	10-Jun-2024	8.6	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to break out of its sandbox. **CVE ID: CVE-2024-23299**	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support.apple.com/en-us/HT214085	O-APP-MACO-200624/687
N/A	10-Jun-2024	5.5	The issue was addressed with improved restriction of data container access. This issue is fixed in macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to access sensitive user data. **CVE ID: CVE-2023-40389**	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214085	O-APP-MACO-200624/688
Affected Version(s): From (including) 14.0 Up to (excluding) 14.4					
N/A	10-Jun-2024	8.6	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Ventura 13.6.5, macOS Monterey	https://support.apple.com/en-us/HT214083, https://support.apple.com/en-us/HT214084, https://support	O-APP-MACO-200624/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.7.4. An app may be able to break out of its sandbox. **CVE ID: CVE-2024-23299**	.apple.com/en-us/HT214085	
Vendor: Canonical					
Product: ubuntu_linux					
Affected Version(s): 18.04					
N/A	04-Jun-2024	7.8	Apport does not disable python crash handler before entering chroot **CVE ID: CVE-2022-28657**	N/A	O-CAN-UBUN-200624/690
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.1	is_closing_session() allows users to create arbitrary tcp dbus connections **CVE ID: CVE-2022-28655**	N/A	O-CAN-UBUN-200624/691
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	04-Jun-2024	5.5	~/.config/apport/settings parsing is vulnerable to "billion laughs" attack **CVE ID: CVE-2022-28652**	N/A	O-CAN-UBUN-200624/692
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to fill up apport.log **CVE ID: CVE-2022-28654**	N/A	O-CAN-UBUN-200624/693
Allocation of	04-Jun-2024	5.5	is_closing_session() allows users to	N/A	O-CAN-UBUN-200624/694

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resources Without Limits or Throttling			consume RAM in the Apport process **CVE ID: CVE-2022-28656**		
N/A	04-Jun-2024	5.5	Apport argument parsing mishandles filename splitting on older kernels resulting in argument spoofing **CVE ID: CVE-2022-28658**	N/A	O-CAN-UBUN-200624/695
Affected Version(s): 20.04					
N/A	04-Jun-2024	7.8	Apport does not disable python crash handler before entering chroot **CVE ID: CVE-2022-28657**	N/A	O-CAN-UBUN-200624/696
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.1	is_closing_session() allows users to create arbitrary tcp dbus connections **CVE ID: CVE-2022-28655**	N/A	O-CAN-UBUN-200624/697
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	04-Jun-2024	5.5	~/.config/apport/settings parsing is vulnerable to "billion laughs" attack **CVE ID: CVE-2022-28652**	N/A	O-CAN-UBUN-200624/698
Allocation of Resources Without	04-Jun-2024	5.5	is_closing_session() allows users to fill up apport.log	N/A	O-CAN-UBUN-200624/699

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			**CVE ID: CVE-2022-28654**		
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to consume RAM in the Apport process **CVE ID: CVE-2022-28656**	N/A	O-CAN-UBUN-200624/700
N/A	04-Jun-2024	5.5	Apport argument parsing mishandles filename splitting on older kernels resulting in argument spoofing **CVE ID: CVE-2022-28658**	N/A	O-CAN-UBUN-200624/701
Affected Version(s): 21.10					
N/A	04-Jun-2024	7.8	Apport does not disable python crash handler before entering chroot **CVE ID: CVE-2022-28657**	N/A	O-CAN-UBUN-200624/702
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.1	is_closing_session() allows users to create arbitrary tcp dbus connections **CVE ID: CVE-2022-28655**	N/A	O-CAN-UBUN-200624/703
Improper Restriction of Recursive Entity References in DTDs ('XML Entity	04-Jun-2024	5.5	~/.config/apport/settings parsing is vulnerable to "billion laughs" attack **CVE ID: CVE-2022-28652**	N/A	O-CAN-UBUN-200624/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Expansion')					
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to fill up apport.log **CVE ID: CVE-2022-28654**	N/A	O-CAN-UBUN-200624/705
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to consume RAM in the Apport process **CVE ID: CVE-2022-28656**	N/A	O-CAN-UBUN-200624/706
N/A	04-Jun-2024	5.5	Apport argument parsing mishandles filename splitting on older kernels resulting in argument spoofing **CVE ID: CVE-2022-28658**	N/A	O-CAN-UBUN-200624/707
Affected Version(s): 22.04					
N/A	04-Jun-2024	7.8	Apport does not disable python crash handler before entering chroot **CVE ID: CVE-2022-28657**	N/A	O-CAN-UBUN-200624/708
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.1	is_closing_session() allows users to create arbitrary tcp dbus connections **CVE ID: CVE-2022-28655**	N/A	O-CAN-UBUN-200624/709
Improper Restriction of Recursive	04-Jun-2024	5.5	~/.config/apport/settings parsing is vulnerable to	N/A	O-CAN-UBUN-200624/710

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Entity References in DTDs ('XML Entity Expansion')			"billion laughs" attack **CVE ID: CVE-2022-28652**		
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to fill up apport.log **CVE ID: CVE-2022-28654**	N/A	O-CAN-UBUN-200624/711
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to consume RAM in the Apport process **CVE ID: CVE-2022-28656**	N/A	O-CAN-UBUN-200624/712
N/A	04-Jun-2024	5.5	Apport argument parsing mishandles filename splitting on older kernels resulting in argument spoofing **CVE ID: CVE-2022-28658**	N/A	O-CAN-UBUN-200624/713
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Out-of-bounds Read	05-Jun-2024	8.1	An out-of-bounds read in the 'bson' module of PyMongo 4.6.2 or earlier allows deserialization of malformed BSON provided by a Server to raise an exception which may contain	https://jira.mongodb.org/browse/PYTHON-4305	O-DEB-DEBI-200624/714

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary application memory. **CVE ID: CVE-2024-5629**		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 40					
Improper Encoding or Escaping of Output	09-Jun-2024	8.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874 does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell. **CVE ID: CVE-2024-5585**	N/A	O-FED-FEDO-200624/715
Observable Discrepancy	09-Jun-2024	5.9	The openssl_private_decrypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_	N/A	O-FED-FEDO-200624/716

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PADDING, which is the default), is vulnerable to the Marvin Attack unless it is used with an OpenSSL version that includes the changes from this pull request: https://github.com/openssl/openssl/pull/13817 (rsa_pkcs1_implicit_rejection). These changes are part of OpenSSL 3.2 and have also been backported to stable versions of various Linux distributions, as well as to the PHP builds provided for Windows since the previous release. All distributors and builders should ensure that this version is used to prevent PHP from being vulnerable. PHP Windows builds for the versions 8.1.29, 8.2.20 and 8.3.8 and above include OpenSSL patches that fix the vulnerability. **CVE ID: CVE-2024-2408**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. **CVE ID: CVE-2024-5458**	https://github.com/php/php-src/security/advisories/GHSA-w8qr-v226-r27w	O-FED-FEDO-200624/717
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	13-Jun-2024	7.8	there is a possible way to bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://source.android.com/security/bulletin/pixel/2024-06-01	O-GOO-ANDR-200624/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. **CVE ID: CVE-2024-32896**		
Vendor: IBM					
Product: i					
Affected Version(s): 7.2					
Observable Discrepancy	07-Jun-2024	5.3	IBM i 7.2, 7.3, 7.4, and 7.5 Service Tools Server (SST) is vulnerable to SST user enumeration by a remote attacker. This vulnerability can be used by a malicious actor to gather information about SST users that can be targeted in further attacks. IBM X-Force ID: 287538. **CVE ID: CVE-2024-31878**	https://exchange.xforce.ibmcloud.com/vulnerabilities/287538, https://www.ibm.com/support/pages/node/7156725	O-IBM-I-200624/719
Affected Version(s): 7.3					
Observable Discrepancy	07-Jun-2024	5.3	IBM i 7.2, 7.3, 7.4, and 7.5 Service Tools Server (SST) is vulnerable to SST user enumeration by a remote attacker. This vulnerability can be used by a malicious actor to gather information about SST users that can be targeted in further attacks.	https://exchange.xforce.ibmcloud.com/vulnerabilities/287538, https://www.ibm.com/support/pages/node/7156725	O-IBM-I-200624/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 287538. **CVE ID: CVE-2024-31878**		
Affected Version(s): 7.4					
Observable Discrepancy	07-Jun-2024	5.3	IBM i 7.2, 7.3, 7.4, and 7.5 Service Tools Server (SST) is vulnerable to SST user enumeration by a remote attacker. This vulnerability can be used by a malicious actor to gather information about SST users that can be targeted in further attacks. IBM X-Force ID: 287538. **CVE ID: CVE-2024-31878**	https://exchange.xforce.ibmcloud.com/vulnerabilities/287538, https://www.ibm.com/support/pages/node/7156725	O-IBM-I-200624/721
Affected Version(s): 7.5					
Observable Discrepancy	07-Jun-2024	5.3	IBM i 7.2, 7.3, 7.4, and 7.5 Service Tools Server (SST) is vulnerable to SST user enumeration by a remote attacker. This vulnerability can be used by a malicious actor to gather information about SST users that can be targeted in further attacks. IBM X-Force ID: 287538.	https://exchange.xforce.ibmcloud.com/vulnerabilities/287538, https://www.ibm.com/support/pages/node/7156725	O-IBM-I-200624/722

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-31878		
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): 6.10.0					
Use After Free	10-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: fix __dst_negative_advice() race __dst_negative_advice() does not enforce proper RCU rules when sk->dst_cache must be cleared, leading to possible UAF. RCU rules are that we must first clear sk->sk_dst_cache, then call dst_release(old_dst). Note that sk_dst_reset(sk) is implementing this protocol correctly, while __dst_negative_advice() uses the wrong order. Given that ip6_negative_advice() has special logic against RTF_CACHE, this means each of the	https://git.kernel.org/stable/c/92f1655aa2b2294d0b49925f3b875a634bd3b59e, https://git.kernel.org/stable/c/b8af8e6118a6605f0e495a58d591ca94a85a50fc	O-LIN-LINU-200624/723

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			three ->negative_advice() existing methods must perform the sk_dst_reset() themselves. Note the check against NULL dst is centralized in __dst_negative_advice(), there is no need to duplicate it in various callbacks. Many thanks to Clement Lecigne for tracking this issue. This old bug became visible after the blamed commit, using UDP sockets. **CVE ID: CVE-2024-36971**		
Affected Version(s): From (including) 4.6 Up to (excluding) 6.9.4					
Use After Free	10-Jun-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: fix __dst_negative_advice() race __dst_negative_advice() does not enforce proper RCU rules when	https://git.kernel.org/stable/c/92f1655aa2b2294d0b49925f3b875a634bd3b59e, https://git.kernel.org/stable/c/b8af8e6118a6605f0e495a58d591ca94a85a50fc	O-LIN-LINU-200624/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sk->dst_cache must be cleared, leading to possible UAF. RCU rules are that we must first clear sk->sk_dst_cache, then call dst_release(old_dst). Note that sk_dst_reset(sk) is implementing this protocol correctly, while __dst_negative_advi ce() uses the wrong order. Given that ip6_negative_advic e() has special logic against RTF_CACHE, this means each of the three ->negative_advice() existing methods must perform the sk_dst_reset() themselves. Note the check against NULL dst is centralized in __dst_negative_advi ce(), there is no need to duplicate		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it in various callbacks. Many thanks to Clement Lecigne for tracking this issue. This old bug became visible after the blamed commit, using UDP sockets. **CVE ID: CVE-2024-36971**		
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	10-Jun-2024	7	A sym-linked file accessed via the repair function in Avast Antivirus <24.2 on Windows may allow user to elevate privilege to delete arbitrary files or run processes as NT AUTHORITY\SYSTEM. The vulnerability exists within the "Repair" (settings -> troubleshooting -> repair) feature, which attempts to delete a file in the current user's AppData directory as NT AUTHORITY\SYST	N/A	O-MIC-WIND-200624/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EM. A low-privileged user can make a pseudo-symlink and a junction folder and point to a file on the system. This can provide a low-privileged user an Elevation of Privilege to win a race-condition which will re-create the system files and make Windows callback to a specially-crafted file which could be used to launch a privileged shell instance. This issue affects Avast Antivirus prior to 24.2. **CVE ID: CVE-2024-5102**		
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.20680					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/726
Product: windows_10_1607					
Affected Version(s): * Up to (excluding) 10.0.14393.7070					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code	https://msrc.microsoft.com/update-	O-MIC-WIND-200624/727

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID: CVE-2024-30080**	guide/vulnerability/CVE-2024-30080	
Product: windows_10_1809					
Affected Version(s): * Up to (excluding) 10.0.17763.5936					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/728
Product: windows_10_21h1					
Affected Version(s): * Up to (excluding) 10.0.19043.4529					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/729
Product: windows_11_21h2					
Affected Version(s): * Up to (excluding) 10.0.22000.3019					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/730
Product: windows_11_22h2					
Affected Version(s): * Up to (excluding) 10.0.22621.3737					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-200624/731

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-30080	lity/CVE-2024-30080	
Product: windows_11_23h2					
Affected Version(s): * Up to (excluding) 10.0.22631.3737					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/732
Product: windows_server_2008					
Affected Version(s): -					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/733
Affected Version(s): r2					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/734
Product: windows_server_2012					
Affected Version(s): -					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/735
Affected Version(s): r2					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/736
Product: windows_server_2016					
Affected Version(s): -					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/737
Product: windows_server_2019					
Affected Version(s): * Up to (excluding) 10.0.17763.5936					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/738
Product: windows_server_2022					
Affected Version(s): * Up to (excluding) 10.0.20348.2522					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080	O-MIC-WIND-200624/739
Product: windows_server_2022_23h2					
Affected Version(s): * Up to (excluding) 10.0.25398.950					
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ)	https://msrc.microsoft.com/up	O-MIC-WIND-200624/740

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID: CVE-2024-30080**	date-guide/vulnerability/CVE-2024-30080	
Vendor: Mitel					
Product: 6869i_sip_firmware					
Affected Version(s): * Up to (including) 4.5.0.41					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Jun-2024	8.8	An issue was discovered on Mitel 6869i through 4.5.0.41 and 5.x through 5.0.0.1018 devices. A command injection vulnerability exists in the hostname parameter taken in by the provis.html endpoint. The provis.html endpoint performs no sanitization on the hostname parameter (sent by an authenticated user), which is subsequently written to disk. During boot, the hostname parameter is executed as part of a series of shell commands. Attackers can achieve remote code execution in the root context by placing shell metacharacters in	N/A	O-MIT-6869-200624/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the hostname parameter. **CVE ID: CVE-2024-37569**		
Affected Version(s): 4.5.0.41					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Jun-2024	8.8	On Mitel 6869i 4.5.0.41 devices, the Manual Firmware Update (upgrade.html) page does not perform sanitization on the username and path parameters (sent by an authenticated user) before appending flags to the busybox ftpget command. This leads to $() command execution. **CVE ID: CVE-2024-37570**	N/A	O-MIT-6869-200624/742
Affected Version(s): From (including) 5.0.0.0 Up to (including) 5.0.0.1018					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Jun-2024	8.8	An issue was discovered on Mitel 6869i through 4.5.0.41 and 5.x through 5.0.0.1018 devices. A command injection vulnerability exists in the hostname parameter taken in by the provis.html endpoint. The provis.html endpoint performs no sanitization on the hostname	N/A	O-MIT-6869-200624/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter (sent by an authenticated user), which is subsequently written to disk. During boot, the hostname parameter is executed as part of a series of shell commands. Attackers can achieve remote code execution in the root context by placing shell metacharacters in the hostname parameter. **CVE ID: CVE-2024-37569**		
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 7.0					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/744
Affected Version(s): 8.0					
Insufficient Verification of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE-200624/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**		
Affected Version(s): 9.0					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/746
Product: enterprise_linux_eus					
Affected Version(s): 8.4					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/747
Affected Version(s): 8.8					
Insufficient Verification of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE-200624/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**		
Affected Version(s): 9.2					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/749
Product: enterprise_linux_for_arm_64					
Affected Version(s): 8.0_aarch64					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/750
Affected Version(s): 8.8_aarch64					
Insufficient Verification of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE-200624/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**		
Affected Version(s): 9.2_aarch64					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/752
Affected Version(s): 9.4_aarch64					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/753
Product: enterprise_linux_for_ibm_z_systems					
Affected Version(s): 8.0_s390x					
Insufficient Verification of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE-200624/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**		
Affected Version(s): 9.2_s390x					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/755
Affected Version(s): 9.4_s390x					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/756
Product: enterprise_linux_for_ibm_z_systems_eus					
Affected Version(s): 8.8_s390x					
Insufficient Verification of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE-200624/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**		
Product: enterprise_linux_for_power_little_endian_eus					
Affected Version(s): 8.0_ppc64le					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/758
Affected Version(s): 8.4_ppc64le					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/759
Affected Version(s): 8.8_ppc64le					
Insufficient Verification of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE-200624/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**		
Affected Version(s): 9.2_ppc64le					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/761
Affected Version(s): 9.4_ppc64le					
Insufficient Verification of Data Authenticity	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**	N/A	O-RED-ENTE-200624/762
Product: enterprise_linux_server_update_services_for_sap_solutions					
Affected Version(s): 8.4					
Insufficient Verification of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE-200624/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server. **CVE ID: CVE-2024-3049**		
Vendor: Samsung					
Product: exynos_1080_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/765
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/766

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/767
Product: exynos_1280_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor,	https://semiconductor.samsung.com/support/quality-	O-SAM-EXYN-200624/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	support/product-security-updates/	
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/770
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and	https://semiconductor.samsung.com/support/quality-support/produc	O-SAM-EXYN-200624/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	t-security-updates/	
Product: exynos_1330_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/772

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/773
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/774

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/775

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: exynos_1380_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/776
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/777

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/778

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/779
Product: exynos_2100_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/781
Missing Encryption	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile	https://semiconductor.samsung.com/support/q	O-SAM-EXYN-200624/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	uality-support/product-security-updates/	
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**		
Product: exynos_2200_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/784
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor,	https://semiconductor.samsung.com/support/quality-support/produc	O-SAM-EXYN-200624/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	t-security-updates/	
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/787
Product: exynos_2400_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
Product: exynos_850_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control)	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/789

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/790
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/791

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/792

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: exynos_9110_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/793
Product: exynos_980_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to disclosure of sensitive information. **CVE ID: CVE-2023-49928**		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/796
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/797

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**		
Product: exynos_9820_firmware					
Affected Version(s): -					
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-49928		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/799
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/800

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**		
Product: exynos_9825_firmware					
Affected Version(s): -					
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/801
Missing Encryption	05-Jun-2024	5.3	An issue was discovered in	https://semiconductor.samsung	O-SAM-EXYN-200624/802

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	.com/support/quality-support/product-security-updates/	
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/803

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**		
Product: exynos_990_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/804
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive	https://semiconductor.samsung.com/support/quality-support/produc	O-SAM-EXYN-200624/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	t-security-updates/	
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/807
Product: exynos_auto_t5123_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
Product: exynos_modem_5123_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/809

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/810
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable	https://semiconductor.samsung.com/support/quality-support/produc	O-SAM-EXYN-200624/811

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. **CVE ID: CVE-2023-49927**	t-security-updates/	
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/812

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-50803		
Product: exynos_modem_5300_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/813
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. **CVE ID: CVE-2023-49928**		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a lack of encryption. **CVE ID: CVE-2023-49927**		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. **CVE ID: CVE-2023-50803**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/816
Product: exynos_w920_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330,	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
Product: exynos_w930_firmware					
Affected Version(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-200624/818

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to disclosure of sensitive information. **CVE ID: CVE-2024-29152**		
Vendor: Tendacn					
Product: o3v2_firmware					
Affected Version(s): 1.0.0.12\\(3880\\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Jun-2024	9.8	Tenda O3V2 v1.0.0.12(3880) was discovered to contain a Blind Command Injection via stpEn parameter in the SetStp function. This vulnerability allows attackers to execute arbitrary commands with root privileges. **CVE ID: CVE-2024-36604**	N/A	O-TEN-O3V2-200624/819
Vendor: uniview					
Product: nvr301-04s2-p4_firmware					
Affected Version(s): * Up to (excluding) nvr-b3801.20.17.240507					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Jun-2024	5.4	Uniview NVR301-04S2-P4 is vulnerable to reflected cross-site scripting attack (XSS). An attacker could send a user a URL that if clicked on could execute malicious JavaScript in their browser. This vulnerability also requires	N/A	O-UNI-NVR3-200624/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication before it can be exploited, so the scope and severity is limited. Also, even if JavaScript is executed, no additional benefits are obtained. **CVE ID: CVE-2024-3850**		
Vendor: vw					
Product: id.charger_connect_firmware					
Affected Version(s): spr3.2					
Insufficient Verification of Data Authenticity	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass	N/A	O-VW-ID.C-200624/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism. **CVE ID: CVE-2024-5684**		
Affected Version(s): spr3.51					
Insufficient Verification of Data Authenticity	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit	N/A	O-VW-ID.C-200624/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability to bypass the authentication mechanism. **CVE ID: CVE-2024-5684**		
Affected Version(s): spr3.52					
Insufficient Verification of Data Authenticity	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism.	N/A	O-VW-ID.C-200624/823

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-5684		
Product: id.charger_pro_firmware					
Affected Version(s): spr3.2					
Insufficient Verification of Data Authenticity	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism. **CVE ID: CVE-2024-5684**	N/A	O-VW-ID.C-200624/824

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): spr3.51					
Insufficient Verification of Data Authenticity	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism. **CVE ID: CVE-2024-5684**	N/A	O-VW-ID.C-200624/825
Affected Version(s): spr3.52					
Insufficient Verification of Data	06-Jun-2024	8.8	An attacker with access to the private network	N/A	O-VW-ID.C-200624/826

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			(the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism. **CVE ID: CVE-2024-5684**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions