National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 - 30 Apr 2022 Vol. 09 No. 08

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 10up					
Product: safe_svg					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-22	6.1	The sanitisation step of the Safe SVG WordPress plugin before 1.9.10 can be bypassed by spoofing the content-type in the POST request to upload a file. Exploiting this vulnerability, an attacker will be able to perform the kinds of attacks that this plugin should prevent (mainly XSS, but depending on further use of uploaded SVG files potentially other XML attacks). **CVE ID : CVE-2022-1091**	https://github.com/10up/safe-svg/pull/28	A-10U-SAFE-040522/1
Vendor: abacus					
Product: abacus_erp_2018					
Improper Authentication	19-Apr-22	8.8	A vulnerability within the authentication process of Abacus ERP allows a remote attacker to bypass the second authentication factor. This issue affects: Abacus ERP v2022 versions prior to R1 of 2022-01-15; v2021 versions prior	https://www.redguard.ch/advisories/abacus_mfa_bypass.txt	A-ABA-ABAC-040522/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to R4 of 2022-01-15; v2020 versions prior to R6 of 2022-01-15; v2019 versions later than R5 (service pack); v2018 versions later than R5 (service pack). This issue does not affect: Abacus ERP v2019 versions prior to R5 of 2020-03-15; v2018 versions prior to R7 of 2020-04-15; v2017 version and prior versions and prior versions. **CVE ID : CVE-2022-1065**		
Product: abacus_erp_2019					
Improper Authentication	19-Apr-22	8.8	A vulnerability within the authentication process of Abacus ERP allows a remote attacker to bypass the second authentication factor. This issue affects: Abacus ERP v2022 versions prior to R1 of 2022-01-15; v2021 versions prior to R4 of 2022-01-15; v2020 versions prior to R6 of 2022-01-15; v2019 versions later than R5 (service pack); v2018 versions later than R5 (service pack). This issue does not affect: Abacus ERP	https://www.redguard.ch/advisories/abacus_mfa_bypass.txt	A-ABA-ABAC-040522/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v2019 versions prior to R5 of 2020-03-15; v2018 versions prior to R7 of 2020-04-15; v2017 version and prior versions and prior versions. **CVE ID : CVE-2022-1065**		
Product: abacus_erp_2020					
Improper Authentication	19-Apr-22	8.8	A vulnerability within the authentication process of Abacus ERP allows a remote attacker to bypass the second authentication factor. This issue affects: Abacus ERP v2022 versions prior to R1 of 2022-01-15; v2021 versions prior to R4 of 2022-01-15; v2020 versions prior to R6 of 2022-01-15; v2019 versions later than R5 (service pack); v2018 versions later than R5 (service pack). This issue does not affect: Abacus ERP v2019 versions prior to R5 of 2020-03-15; v2018 versions prior to R7 of 2020-04-15; v2017 version and prior versions and prior versions. **CVE ID : CVE-2022-1065**	https://www.redguard.ch/advisories/abacus_mfa_bypass.txt	A-ABA-ABAC-040522/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: abacus_erp_2021					
Improper Authentication	19-Apr-22	8.8	A vulnerability within the authentication process of Abacus ERP allows a remote attacker to bypass the second authentication factor. This issue affects: Abacus ERP v2022 versions prior to R1 of 2022-01-15; v2021 versions prior to R4 of 2022-01-15; v2020 versions prior to R6 of 2022-01-15; v2019 versions later than R5 (service pack); v2018 versions later than R5 (service pack). This issue does not affect: Abacus ERP v2019 versions prior to R5 of 2020-03-15; v2018 versions prior to R7 of 2020-04-15; v2017 version and prior versions and prior versions. **CVE ID : CVE-2022-1065**	https://www.redguard.ch/advisories/abacus_mfa_bypass.txt	A-ABA-ABAC-040522/5
Product: abacus_erp_2022					
Improper Authentication	19-Apr-22	8.8	A vulnerability within the authentication process of Abacus ERP allows a remote attacker to bypass the second authentication factor. This issue affects:	https://www.redguard.ch/advisories/abacus_mfa_bypass.txt	A-ABA-ABAC-040522/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Abacus ERP v2022 versions prior to R1 of 2022-01-15; v2021 versions prior to R4 of 2022-01-15; v2020 versions prior to R6 of 2022-01-15; v2019 versions later than R5 (service pack); v2018 versions later than R5 (service pack). This issue does not affect: Abacus ERP v2019 versions prior to R5 of 2020-03-15; v2018 versions prior to R7 of 2020-04-15; v2017 version and prior versions and prior versions. **CVE ID : CVE-2022-1065**		
Vendor: accesspressthemes					
Product: access_demo_importer					
Cross-Site Request Forgery (CSRF)	18-Apr-22	6.5	Cross-Site Request Forgery (CSRF) in Access Demo Importer <= 1.0.7 on WordPress allows an attacker to activate any installed plugin. **CVE ID : CVE-2022-23975**	https://wordpress.org/plugins/access-demo-importer/#developers	A-ACC-ACCE-040522/7
Cross-Site Request Forgery (CSRF)	18-Apr-22	8.1	Cross-Site Request Forgery (CSRF) in Access Demo Importer <= 1.0.7 on WordPress allows an attacker to reset all data (posts / pages / media).	https://wordpress.org/plugins/access-demo-importer/#developers	A-ACC-ACCE-040522/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23976		
Vendor: ad_injection_project					
Product: ad_injection					
Improper Control of Generation of Code ('Code Injection')	18-Apr-22	7.2	The Ad Injection WordPress plugin through 1.2.0.19 does not properly sanitize the body of the adverts injected into the pages, allowing a high privileged user (Admin+) to inject arbitrary HTML or javascript even with unfiltered_html disallowed, leading to a stored cross-site scripting (XSS) vulnerability. Further it is also possible to inject PHP code, leading to a Remote Code execution (RCE) vulnerability, even if the DISALLOW_FILE_EDIT and DISALLOW_FILE_MOD constants are both set. **CVE ID : CVE-2022-0661**	N/A	A-AD_-AD_I-040522/9
Vendor: Apache					
Product: apisix					
Generation of Error Message Containing	20-Apr-22	7.5	In APache APISIX before 3.13.1, the jwt-auth plugin has a security issue that leaks the user's secret key because	https://lists.apache.org/thread/6qpfyxogbvn18g9xr8g218jjfjbfsbhr	A-APA-APIS-040522/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			the error message returned from the dependency lua-resty-jwt contains sensitive information. **CVE ID : CVE-2022-29266**		
Vendor: Atlassian					
Product: bitbucket_data_center					
Deserialization of Untrusted Data	20-Apr-22	9.8	SharedSecretClusterAuthenticator in Atlassian Bitbucket Data Center versions 5.14.0 and later before 7.6.14, 7.7.0 and later prior to 7.17.6, 7.18.0 and later prior to 7.18.4, 7.19.0 and later prior to 7.19.4, and 7.20.0 allow a remote, unauthenticated attacker to execute arbitrary code via Java deserialization. **CVE ID : CVE-2022-26133**	https://jira.atlassian.com/browse/BSERV-13173, https://confluence.atlassian.com/security/multiple-products-security-advisory-hazelcast-vulnerable-to-remote-code-execution-cve-2016-10750-1116292387.html	A-ATL-BITB-040522/11
Product: jira_core					
Improper Authentication	20-Apr-22	9.8	A vulnerability in Jira Seraph allows a remote, unauthenticated attacker to bypass authentication by sending a specially crafted HTTP request. This affects Atlassian Jira Server and Data Center versions before 8.13.18, versions	https://confluence.atlassian.com/display/JIRA/Jira+Security+Advisory+2022-04-20, https://jira.atlassian.com/browse/JSDSERVER-11224, https://jira.atlassian.com/brow	A-ATL-JIRA-040522/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.14.0 and later before 8.20.6, and versions 8.21.0 and later before 8.22.0. This also affects Atlassian Jira Service Management Server and Data Center versions before 4.13.18, versions 4.14.0 and later before 4.20.6, and versions 4.21.0 and later before 4.22.0. **CVE ID : CVE-2022-0540**	se/JRASERVER-73650	
Product: jira_data_center					
Improper Authentication	20-Apr-22	9.8	A vulnerability in Jira Seraph allows a remote, unauthenticated attacker to bypass authentication by sending a specially crafted HTTP request. This affects Atlassian Jira Server and Data Center versions before 8.13.18, versions 8.14.0 and later before 8.20.6, and versions 8.21.0 and later before 8.22.0. This also affects Atlassian Jira Service Management Server and Data Center versions before 4.13.18, versions 4.14.0 and later before 4.20.6, and	https://confluence.atlassian.com/display/JIRA/Jira+Security+Advisory+2022-04-20, https://jira.atlassian.com/browse/JSDSERVER-11224, https://jira.atlassian.com/browse/JRASERVER-73650	A-ATL-JIRA-040522/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 4.21.0 and later before 4.22.0. **CVE ID : CVE-2022-0540**		
Product: jira_server					
Improper Authentication	20-Apr-22	9.8	A vulnerability in Jira Seraph allows a remote, unauthenticated attacker to bypass authentication by sending a specially crafted HTTP request. This affects Atlassian Jira Server and Data Center versions before 8.13.18, versions 8.14.0 and later before 8.20.6, and versions 8.21.0 and later before 8.22.0. This also affects Atlassian Jira Service Management Server and Data Center versions before 4.13.18, versions 4.14.0 and later before 4.20.6, and versions 4.21.0 and later before 4.22.0. **CVE ID : CVE-2022-0540**	https://confluence.atlassian.com/display/JIRA/Jira+Security+Advisory+2022-04-20, https://jira.atlassian.com/browse/JSDSERVER-11224, https://jira.atlassian.com/browse/JRASERVER-73650	A-ATL-JIRA-040522/14
Product: jira_service_management					
Improper Authentication	20-Apr-22	9.8	A vulnerability in Jira Seraph allows a remote, unauthenticated attacker to bypass authentication by sending a specially	https://confluence.atlassian.com/display/JIRA/Jira+Security+Advisory+2022-04-20, https://jira.atla	A-ATL-JIRA-040522/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP request. This affects Atlassian Jira Server and Data Center versions before 8.13.18, versions 8.14.0 and later before 8.20.6, and versions 8.21.0 and later before 8.22.0. This also affects Atlassian Jira Service Management Server and Data Center versions before 4.13.18, versions 4.14.0 and later before 4.20.6, and versions 4.21.0 and later before 4.22.0. **CVE ID : CVE-2022-0540**	ssian.com/browse/JSDSERVER-11224, https://jira.atlassian.com/browse/JRASERVER-73650	
Vendor: attendance_and_payroll_system_project					
Product: attendance_and_payroll_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\employee_delete.php. **CVE ID : CVE-2022-28006**	N/A	A-ATT-ATTE-040522/16
Improper Neutralization of Special Elements used in an SQL Command	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component	N/A	A-ATT-ATTE-040522/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			\admin\cashadvance_delete.php. **CVE ID : CVE-2022-28007**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\attendance_delete.php. **CVE ID : CVE-2022-28008**	N/A	A-ATT-ATTE-040522/18
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\attendance_delete.php. **CVE ID : CVE-2022-28009**	N/A	A-ATT-ATTE-040522/19
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\overtime_delete.php. **CVE ID : CVE-2022-28010**	N/A	A-ATT-ATTE-040522/20
Improper Neutralization of Special Elements	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL	N/A	A-ATT-ATTE-040522/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			injection vulnerability via the component \admin\schedule_delete.php. **CVE ID : CVE-2022-28011**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\position_delete.php. **CVE ID : CVE-2022-28012**	N/A	A-ATT-ATTE-040522/22
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\schedule_employee_edit.php. **CVE ID : CVE-2022-28013**	N/A	A-ATT-ATTE-040522/23
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\attendance_edit.php. **CVE ID : CVE-2022-28014**	N/A	A-ATT-ATTE-040522/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\cashadvance_edit.php. **CVE ID : CVE-2022-28015**	N/A	A-ATT-ATTE-040522/25
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\deduction_edit.php. **CVE ID : CVE-2022-28016**	N/A	A-ATT-ATTE-040522/26
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\overtime_edit.php. **CVE ID : CVE-2022-28017**	N/A	A-ATT-ATTE-040522/27
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\schedule_edit.php.	N/A	A-ATT-ATTE-040522/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28018		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\employee_edit.php. **CVE ID : CVE-2022-28019**	N/A	A-ATT-ATTE-040522/29
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	8.8	Attendance and Payroll System v1.0 was discovered to contain a SQL injection vulnerability via the component \admin\position_edit.php. **CVE ID : CVE-2022-28020**	N/A	A-ATT-ATTE-040522/30
Vendor: Autodesk					
Product: advance_steel					
Out-of-bounds Write	19-Apr-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write beyond the allocated buffer while parsing JT files. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2022-25788**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0002	A-AUT-ADVA-040522/31
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted PICT, BMP, PSD or TIF file in Autodesk	https://www.autodesk.com/trust/security-	A-AUT-ADVA-040522/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AutoCAD 2022, 2021, 2020, 2019 may be used to write beyond the allocated buffer while parsing PICT, BMP, PSD or TIF file. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27529**	advisories/adsk-sa-2022-0004	
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted TIF or PICT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27530**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-ADVA-040522/33
Product: autocad					
Out-of-bounds Write	19-Apr-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write beyond the allocated buffer while parsing JT files. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2022-25788**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0002	A-AUT-AUTO-040522/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted PICT, BMP, PSD or TIF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 may be used to write beyond the allocated buffer while parsing PICT, BMP, PSD or TIF file. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27529**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/35
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted TIF or PICT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27530**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/36
Product: autocad_architecture					
Out-of-bounds Write	19-Apr-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write beyond the allocated buffer while parsing JT files. This vulnerability can be exploited to execute arbitrary code.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0002	A-AUT-AUTO-040522/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25788		
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted PICT, BMP, PSD or TIF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 may be used to write beyond the allocated buffer while parsing PICT, BMP, PSD or TIF file. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27529**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/38
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted TIF or PICT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27530**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/39
Product: autocad_electrical					
Out-of-bounds Write	19-Apr-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write beyond the allocated buffer while parsing JT files. This vulnerability can be	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0002	A-AUT-AUTO-040522/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited to execute arbitrary code. **CVE ID : CVE-2022-25788**		
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted PICT, BMP, PSD or TIF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 may be used to write beyond the allocated buffer while parsing PICT, BMP, PSD or TIF file. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27529**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/41
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted TIF or PICT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27530**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/42
Product: autocad_lt					
Out-of-bounds Write	19-Apr-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write beyond the allocated buffer while parsing JT files. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0002	A-AUT-AUTO-040522/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2022-25788**		
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted PICT, BMP, PSD or TIF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 may be used to write beyond the allocated buffer while parsing PICT, BMP, PSD or TIF file. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27529**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/44
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted TIF or PICT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27530**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/45
Product: autocad_map_3d					
Out-of-bounds Write	19-Apr-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write beyond the allocated buffer while parsing	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0002	A-AUT-AUTO-040522/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JT files. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2022-25788**		
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted PICT, BMP, PSD or TIF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 may be used to write beyond the allocated buffer while parsing PICT, BMP, PSD or TIF file. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27529**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/47
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted TIF or PICT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27530**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/48
Product: autocad_mechanical					
Out-of-bounds Write	19-Apr-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write beyond the allocated	https://www.autodesk.com/trust/security-	A-AUT-AUTO-040522/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer while parsing JT files. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2022-25788**	advisories/adsk-sa-2022-0002	
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted PICT, BMP, PSD or TIF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 may be used to write beyond the allocated buffer while parsing PICT, BMP, PSD or TIF file. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27529**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/50
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted TIF or PICT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27530**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/51
Product: autocad_mep					
Out-of-bounds Write	19-Apr-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write	https://www.autodesk.com/trust/security-	A-AUT-AUTO-040522/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beyond the allocated buffer while parsing JT files. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2022-25788**	advisories/adsk-sa-2022-0002	
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted PICT, BMP, PSD or TIF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 may be used to write beyond the allocated buffer while parsing PICT, BMP, PSD or TIF file. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27529**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/53
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted TIF or PICT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27530**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/54
Product: autocad_plant_3d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Apr-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write beyond the allocated buffer while parsing JT files. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2022-25788**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0002	A-AUT-AUTO-040522/55
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted PICT, BMP, PSD or TIF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 may be used to write beyond the allocated buffer while parsing PICT, BMP, PSD or TIF file. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27529**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/56
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted TIF or PICT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27530**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-040522/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: civil_3d					
Out-of-bounds Write	19-Apr-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write beyond the allocated buffer while parsing JT files. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2022-25788**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0002	A-AUT-CIVI-040522/58
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted PICT, BMP, PSD or TIF file in Autodesk AutoCAD 2022, 2021, 2020, 2019 may be used to write beyond the allocated buffer while parsing PICT, BMP, PSD or TIF file. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27529**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-CIVI-040522/59
Out-of-bounds Write	18-Apr-22	7.8	A maliciously crafted TIF or PICT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to write beyond the allocated buffer through Buffer overflow vulnerability. This vulnerability may be exploited to execute arbitrary code.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-CIVI-040522/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27530		
Product: design_review					
Out-of-bounds Write	18-Apr-22	7.8	A malicious crafted .dwf file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current proces. **CVE ID : CVE-2022-27525**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-040522/61
Out-of-bounds Write	18-Apr-22	7.8	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-27526**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-DESI-040522/62
Product: inventor					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Apr-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022 may be used to write beyond the allocated buffer while parsing JT files. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2022-25788**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0002	A-AUT-INVE-040522/63
Product: navisworks					
Out-of-bounds Write	19-Apr-22	7.8	A Memory Corruption vulnerability may lead to code execution through maliciously crafted DLL files. It was fixed in PDFTron earlier than 9.0.7 version in Autodesk Navisworks 2022. **CVE ID : CVE-2022-27527**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2021-0010	A-AUT-NAVI-040522/64
Vendor: autolinks_project					
Product: autolinks					
Cross-Site Request Forgery (CSRF)	18-Apr-22	5.4	The Autolinks WordPress plugin through 1.0.1 does not have CSRF check in place when updating its settings, and does not sanitise as well as escape them, which could allow attackers to perform Stored Cross-Site scripting against a logged in	N/A	A-AUT-AUTO-040522/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin via a CSRF attack **CVE ID : CVE-2022-1112**		
Vendor: automatedlogic					
Product: webctrl_server					
URL Redirection to Untrusted Site ('Open Redirect')	19-Apr-22	6.1	Automated Logic's WebCtrl Server Version 6.1 'Help' index pages are vulnerable to open redirection. The vulnerability allows an attacker to send a maliciously crafted URL which could result in redirecting the user to a malicious webpage or downloading a malicious file. **CVE ID : CVE-2022-1019**	https://www.corporate.carrier.com/Images/CARR-PSA-ALC-WebCTRL-001-1121_tcm558-149395.pdf	A-AUT-WEBC-040522/66
Vendor: automatic_question_paper_generator_project					
Product: automatic_question_paper_generator					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-22	9.8	Automatic Question Paper Generator v1.0 contains a Time-Based Blind SQL injection vulnerability via the id GET parameter. **CVE ID : CVE-2022-26631**	https://github.com/Cyb3rR3ap3r/CVE-2022-26631	A-AUT-AUTO-040522/67
Vendor: baby_care_system_project					
Product: baby_care_system					
Improper Neutralization of Special Elements	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection	N/A	A-BAB-BABY-040522/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			vulnerability via BabyCare/admin.php?id=theme&setid=. **CVE ID : CVE-2022-28420**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin.php?id=posts&action=display&value=1&postid=. **CVE ID : CVE-2022-28421**	N/A	A-BAB-BABY-040522/69
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/posts.php&action=edit. **CVE ID : CVE-2022-28422**	N/A	A-BAB-BABY-040522/70
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/posts.php&action=delete. **CVE ID : CVE-2022-28423**	N/A	A-BAB-BABY-040522/71
Improper Neutralization of Special Elements used in an SQL Command	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/posts.php&find=.	N/A	A-BAB-BABY-040522/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2022-28424**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/pagerole.php&action=display&value=1&roleid=. **CVE ID : CVE-2022-28425**	N/A	A-BAB-BABY-040522/73
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/pagerole.php&action=edit&roleid=. **CVE ID : CVE-2022-28426**	N/A	A-BAB-BABY-040522/74
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/inbox.php&action=read&msgid=. **CVE ID : CVE-2022-28427**	N/A	A-BAB-BABY-040522/75
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/inbox.php&action=delete&msgid=. **CVE ID : CVE-2022-28429**	N/A	A-BAB-BABY-040522/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/siteoptions.php&social=remove&sid=2. **CVE ID : CVE-2022-28431**	N/A	A-BAB-BABY-040522/77
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin.php?id=siteoptions&social=display&value=0&sid=2. **CVE ID : CVE-2022-28432**	N/A	A-BAB-BABY-040522/78
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=display&value=Show&userid=. **CVE ID : CVE-2022-28433**	N/A	A-BAB-BABY-040522/79
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin.php?id=siteoptions&social=edit&sid=2. **CVE ID : CVE-2022-28434**	N/A	A-BAB-BABY-040522/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/siteoptions.php&action=displaygoal&value=1&roleid=1. **CVE ID : CVE-2022-28435**	N/A	A-BAB-BABY-040522/81
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=display&value=Hide&userid=. **CVE ID : CVE-2022-28436**	N/A	A-BAB-BABY-040522/82
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=type&userrole=Admin&userid=3. **CVE ID : CVE-2022-28437**	N/A	A-BAB-BABY-040522/83
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=type&userrole=User&userid=. **CVE ID : CVE-2022-28438**	N/A	A-BAB-BABY-040522/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&&action=delete&userid=4. **CVE ID : CVE-2022-28439**	N/A	A-BAB-BABY-040522/85
Vendor: blazer_project					
Product: blazer					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	7.5	Blazer before 2.6.0 allows SQL Injection. In certain circumstances, an attacker could get a user to run a query they would not have normally run. **CVE ID : CVE-2022-29498**	N/A	A-BLA-BLAZ-040522/86
Vendor: bwm-ng_project					
Product: bwm-ng					
NULL Pointer Dereference	18-Apr-22	7.5	An issue was discovered in in bwm-ng v0.6.2. An arbitrary null write exists in get_cmdln_options() function in src/options.c. **CVE ID : CVE-2022-1341**	https://github.com/vgropp/bwm-ng/commit/9774f23bf78a6e6d3ae4cfe3d73bad34f2fdcd17	A-BWM-BWM--040522/87
Vendor: calderaforms					
Product: caldera_forms					
Improper Neutralization of Input During Web	18-Apr-22	6.1	The Caldera Forms WordPress plugin before 1.9.7 does not validate and escape	N/A	A-CAL-CALD-040522/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			the cf-api parameter before outputting it back in the response, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-0879**		
Vendor: car_driving_school_management_system_project					
Product: car_driving_school_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Car Driving School Managment System v1.0 was discovered to contain a SQL injection vulnerability via /cdsms/classes/Master.php?f=delete_package. **CVE ID : CVE-2022-28412**	N/A	A-CAR-CAR_-040522/89
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Car Driving School Management System v1.0 was discovered to contain a SQL injection vulnerability via /cdsms/classes/Master.php?f=delete_enrollment. **CVE ID : CVE-2022-28413**	N/A	A-CAR-CAR_-040522/90
Vendor: chatwoot					
Product: chatwoot					
Improper Neutralization of Input During Web Page Generation	21-Apr-22	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository chatwoot/chatwoot prior to 2.5.0. **CVE ID : CVE-2022-1022**	https://github.com/chatwoot/chatwoot/commit/27ddd77a1b621f503fe89a436a49f44b0b1204b5, https://huntr.d	A-CHA-CHAT-040522/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				ev/bounties/2e4ac6b5-7357-415d-9633-65c636b20e94	
Vendor: cleantalk					
Product: antispam					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Apr-22	6.1	The CleanTalk AntiSpam plugin <= 5.173 for WordPress is vulnerable to Reflected Cross-Site Scripting (XSS) via the $_REQUEST['page'] parameter in`/lib/Cleantalk/ApbctWP/FindSpam/ListTable/Comments.php` **CVE ID : CVE-2022-28221**	https://www.wordfence.com/blog/2022/03/reflected-xss-in-spam-protection-antispam-firewall-by-cleantalk/	A-CLE-ANTI-040522/92
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Apr-22	6.1	The CleanTalk AntiSpam plugin <= 5.173 for WordPress is vulnerable to Reflected Cross-Site Scripting (XSS) via the $_REQUEST['page'] parameter in`/lib/Cleantalk/ApbctWP/FindSpam/ListTable/Users.php` **CVE ID : CVE-2022-28222**	N/A	A-CLE-ANTI-040522/93
Vendor: codeastrology					
Product: woo_product_table					
Cross-Site Request Forgery (CSRF)	18-Apr-22	9.8	The Product Table for WooCommerce (wooproducttable) WordPress plugin	N/A	A-COD-WOO_-040522/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 3.1.2 does not have authorisation and CSRF checks in the wpt_admin_update_notice_option AJAX action (available to both unauthenticated and authenticated users), as well as does not validate the callback parameter, allowing unauthenticated attackers to call arbitrary functions with either none or one user controlled argument **CVE ID : CVE-2022-1020**		
Vendor: Combodo					
Product: itop					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Apr-22	5.4	Combodo iTop is a web based IT Service Management tool. In 3.0.0 beta releases prior to 3.0.0 beta3 a malicious script can be injected in tooltips using iTop customization mechanism. This provides a stored cross site scripting attack vector to authorized users of the system. Users are advised to upgrade. There are no known workarounds for this issue.	https://www.github.com/combodo/itop/commit/ebbf6e56befda2070b00d68c7c3e531a6ce6b59e, https://github.com/Combodo/iTop/security/advisories/GHSA-29h7-jw2p-pcw3	A-COM-ITOP-040522/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24870		
Vendor: contest-gallery					
Product: contest_gallery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-22	4.8	Authenticated (author or higher role) Stored Cross-Site Scripting (XSS) in Contest Gallery (WordPress plugin) <= 13.1.0.9 **CVE ID : CVE-2022-27853**	https://patchstack.com/database/vulnerability/contest-gallery/wordpress-contest-gallery-plugin-13-1-0-9-authenticated-stored-cross-site-scripting-xss-vulnerability, https://wordpress.org/plugins/contest-gallery/	A-CON-CONT-040522/96
Vendor: contextureintl					
Product: page_security_\&_membership					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-22	4.8	The Page Security & Membership WordPress plugin through 1.5.15 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2022-1088**	N/A	A-CON-PAGE-040522/97
Vendor: crypt-server_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: crypt-server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-22	6.1	Crypt Server before 3.3.0 allows XSS in the index view. This is related to serial, computername, and username. **CVE ID : CVE-2022-29589**	https://github.com/grahamgilbert/Crypt-Server/pull/109	A-CRY-CRYP-040522/98
Vendor: cybelsoft					
Product: thinvnc					
Improper Authentication	18-Apr-22	10	ThinVNC version 1.0b1 allows an unauthenticated user to bypass the authentication process via 'http://thin-vnc:8080/cmd?cmd=connect' by obtaining a valid SID without any kind of authentication. It is possible to achieve code execution on the server by sending keyboard or mouse events to the server. **CVE ID : CVE-2022-25226**	N/A	A-CYB-THIN-040522/99
Vendor: daily_prayer_time_project					
Product: daily_prayer_time					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-22	9.8	The Daily Prayer Time WordPress plugin before 2022.03.01 does not sanitise and escape the month parameter before using it in a SQL statement via the	N/A	A-DAI-DAIL-040522/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			get_monthly_timetable AJAX action (available to unauthenticated users), leading to an unauthenticated SQL injection **CVE ID : CVE-2022-0785**		
Vendor: databasir_project					
Product: databasir					
Use of Hard-coded Credentials	20-Apr-22	9.8	Databasir is a team-oriented relational database model document management platform. Databasir 1.01 has Use of Hard-coded Cryptographic Key vulnerability. An attacker can use hard coding to generate login credentials of any user and log in to the service background located at different IP addresses. **CVE ID : CVE-2022-24860**	https://github.com/vran-dev/databasir/security/advisories/GHSA-9prp-5jc9-jpgg	A-DAT-DATA-040522/101
Vendor: detekt					
Product: detekt					
Improper Restriction of XML External Entity Reference	21-Apr-22	9.8	Improper Restriction of XML External Entity Reference in GitHub repository detekt/detekt prior to 1.20.0. **CVE ID : CVE-2022-0272**	https://huntr.dev/bounties/23e37ba7-96d5-4037-a90a-8c8f4a70ce44, https://github.com/detekt/detekt/commit/c965a8d2a6bbdb9	A-DET-DETE-040522/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bcfc6acfa7bbffd3da81f5395	
Vendor: ecjia					
Product: daojia					
Incorrect Authorization	19-Apr-22	7.5	** DISPUTED ** ecjia-daojia 1.38.1-20210202629 is vulnerable to information leakage via content/apps/installer/classes/Helper.php. When the web program is installed, a new environment file is created, and the database information is recorded, including the database record password. NOTE: the vendor disputes this because the environment file is in the data directory, which is not intended for access by website visitors (only the statics directory can be accessed by website visitors). **CVE ID : CVE-2022-27055**	N/A	A-ECJ-DAOJ-040522/103
Vendor: elementor					
Product: elementor_website_builder					
Missing Authorization	19-Apr-22	8.8	The Elementor Website Builder plugin for WordPress is vulnerable to unauthorized execution of several AJAX actions due to a	https://plugins.trac.wordpress.org/changeset/2708766/elementor/trunk/core/app/modules	A-ELE-ELEM-040522/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing capability check in the ~/core/app/modules/onboarding/module.php file that make it possible for attackers to modify site data in addition to uploading malicious files that can be used to obtain remote code execution, in versions 3.6.0 to 3.6.2. **CVE ID : CVE-2022-1329**	/onboarding/module.php	
Vendor: fleetdm					
Product: fleet					
Incorrect Authorization	18-Apr-22	8.1	fleetdm/fleet is an open source device management, built on osquery. All versions of fleet making use of the teams feature are affected by this authorization bypass issue. Fleet instances without teams, or with teams but without restricted team accounts are not affected. In affected versions a team admin can erroneously add themselves as admin, maintainer or observer on other teams. Users are advised to upgrade to version 4.13.	https://github.com/fleetdm/fleet/security/advisories/GHSA-pr2g-j78h-84cr, https://github.com/fleetdm/fleet/commit/da171d3b8d149c30b8307723cbe6b6e8847cb30c	A-FLE-FLEE-040522/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There are no known workarounds for this issue. **CVE ID : CVE-2022-24841**		
Vendor: forestblog_project					
Product: forestblog					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Apr-22	6.1	ForestBlog through 2022-02-16 allows admin/profile/save userAvatar XSS during addition of a user avatar. **CVE ID : CVE-2022-29020**	N/A	A-FOR-FORE-040522/106
Vendor: Formalms					
Product: formalms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Apr-22	9.8	An Unauthenticated time-based blind SQL injection vulnerability exists in Forma LMS prior to v.1.4.3. **CVE ID : CVE-2022-27104**	https://www.formalms.org/download.html	A-FOR-FORM-040522/107
Vendor: GIT					
Product: git					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	19-Apr-22	9.8	The package git before 1.11.0 are vulnerable to Command Injection via git argument injection. When calling the fetch(remote = 'origin', opts = {}) function, the remote parameter is passed to the git fetch	https://snyk.io/vuln/SNYK-RUBY-GIT-2421270, https://github.com/ruby-git/ruby-git/pull/569	A-GIT-GIT-040522/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection. **CVE ID : CVE-2022-25648**		
Vendor: git_large_file_storage_project					
Product: git_large_file_storage					
Untrusted Search Path	20-Apr-22	7.8	On Windows, if Git LFS operates on a malicious repository with a `..exe` file as well as a file named `git.exe`, and `git.exe` is not found in `PATH`, the `..exe` program will be executed, permitting the attacker to execute arbitrary code. This does not affect Unix systems. Similarly, if the malicious repository contains files named `..exe` and `cygpath.exe`, and `cygpath.exe` is not found in `PATH`, the `..exe` program will be executed when certain Git LFS commands are run. More generally, if the current working directory contains any file with a base name of `.` and a file extension from `PATHEXT` (except `.bat` and `.cmd`), and	https://github.com/git-lfs/git-lfs/security/advisories/GHSA-6rw3-3whw-jvjj	A-GIT-GIT_-040522/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			also contains another file with the same base name as a program Git LFS intends to execute (such as `git`, `cygpath`, or `uname`) and any file extension from `PATHEXT` (including `.bat` and `.cmd`), then, on Windows, when Git LFS attempts to execute the intended program the `..exe`, `..com`, etc., file will be executed instead, but only if the intended program is not found in any directory listed in `PATH`. The vulnerability occurs because when Git LFS detects that the program it intends to run does not exist in any directory listed in `PATH` then Git LFS passes an empty string as the executable file path to the Go `os/exec` package, which contains a bug such that, on Windows, it prepends the name of the current working directory (i.e., `.`) to the empty string without adding a path separator, and as a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result searches in that directory for a file with the base name `.` combined with any file extension from `PATHEXT`, executing the first one it finds. (The reason `..bat` and `..cmd` files are not executed in the same manner is that, although the Go `os/exec` package tries to execute them just as it does a `..exe` file, the Microsoft Win32 API `CreateProcess()` family of functions have an undocumented feature in that they apparently recognize when a caller is attempting to execute a batch script file and instead run the `cmd.exe` command interpreter, passing the full set of command line arguments as parameters. These are unchanged from the command line arguments set by Git LFS, and as such, the intended program's name is the first, resulting in a command line like		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`cmd.exe /c git`, which then fails.) Git LFS has resolved this vulnerability by always reporting an error when a program is not found in any directory listed in `PATH` rather than passing an empty string to the Go `os/exec` package in this case. The bug in the Go `os/exec` package has been reported to the Go project and is expected to be patched after this security advisory is published. The problem was introduced in version 2.12.1 and is patched in version 3.1.3. Users of affected versions should upgrade to version 3.1.3. There are currently no known workarounds at this time. **CVE ID : CVE-2022-24826**		
Vendor: GNU					
Product: ncurses					
Out-of-bounds Read	18-Apr-22	7.1	ncurses 6.3 before patch 20220416 has an out-of-bounds read and segmentation violation in convert_strings in	https://lists.gnu.org/archive/html/bug-ncurses/2022-04/msg00016.html, https://lists.gn	A-GNU-NCUR-040522/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tinfo/read_entry.c in the terminfo library. **CVE ID : CVE-2022-29458**	u.org/archive/html/bug-ncurses/2022-04/msg00014.html	
Vendor: Golang					
Product: go					
Allocation of Resources Without Limits or Throttling	20-Apr-22	7.5	encoding/pem in Go before 1.17.9 and 1.8.x before 1.8.1 has a Decode stack overflow via a large amount of PEM data. **CVE ID : CVE-2022-24675**	https://groups.google.com/g/golang-announce, https://groups.google.com/g/golang-announce/c/oecdBNLOml8	A-GOL-GO-040522/111
Improper Certificate Validation	20-Apr-22	7.5	Certificate.Verify in crypto/x509 in Go 1.18.x before 1.18.1 can be caused to panic on macOS when presented with certain malformed certificates. This allows a remote TLS server to cause a TLS client to panic. **CVE ID : CVE-2022-27536**	https://groups.google.com/g/golang-announce, https://groups.google.com/g/golang-announce/c/oecdBNLOml8	A-GOL-GO-040522/112
N/A	20-Apr-22	7.5	The generic P-256 feature in crypto/elliptic in Go before 1.17.9 and 1.18.x before 1.18.1 allows a panic via long scalar input. **CVE ID : CVE-2022-28327**	https://groups.google.com/g/golang-announce, https://groups.google.com/g/golang-announce/c/oecdBNLOml8	A-GOL-GO-040522/113
Vendor: good-bad-comments_project					
Product: good-bad-comments					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-22	4.8	The Good & Bad Comments WordPress plugin through 1.0.0 does not sanitise and escape its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2022-1090**	N/A	A-GOO-GOOD-040522/114
Vendor: hashicorp					
Product: consul					
Server-Side Request Forgery (SSRF)	19-Apr-22	7.5	HashiCorp Consul and Consul Enterprise through 2022-04-12 allow SSRF. **CVE ID : CVE-2022-29153**	https://discuss.hashicorp.com, https://discuss.hashicorp.com/t/hcsec-2022-10-consul-s-http-health-check-may-allow-server-side-request-forgery/38393	A-HAS-CONS-040522/115
Vendor: home_owners_collection_management_system_project					
Product: home_owners_collection_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Home Owners Collection Management System v1.0 was discovered to contain a SQL injection vulnerability via /hocms/classes/Mas	N/A	A-HOM-HOME-040522/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ter.php?f=delete_member. **CVE ID : CVE-2022-28414**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Home Owners Collection Management System v1.0 was discovered to contain a SQL injection vulnerability via /hocms/classes/Master.php?f=delete_collection. **CVE ID : CVE-2022-28415**	N/A	A-HOM-HOME-040522/117
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Home Owners Collection Management System v1.0 was discovered to contain a SQL injection vulnerability via /hocms/classes/Master.php?f=delete_phase. **CVE ID : CVE-2022-28416**	N/A	A-HOM-HOME-040522/118
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Home Owners Collection Management System v1.0 was discovered to contain a SQL injection vulnerability via /hocms/classes/Master.php?f=delete_phase. **CVE ID : CVE-2022-28417**	N/A	A-HOM-HOME-040522/119
Vendor: hotdog_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: hotdog					
Improper Privilege Management	19-Apr-22	8.8	Incomplete fix for CVE-2021-3101. Hotdog, prior to v1.0.2, did not mimic the resource limits, device restrictions, or syscall filters of the target JVM process. This would allow a container to exhaust the resources of the host, modify devices, or make syscalls that would otherwise be blocked. **CVE ID : CVE-2022-0071**	https://unit42.paloaltonetworks.com/aws-log4shell-hot-patch-vulnerabilities	A-HOT-HOTD-040522/120
Vendor: http-swagger_project					
Product: http-swagger					
Improper Handling of Exceptional Conditions	18-Apr-22	7.5	http-swagger is an open source wrapper to automatically generate RESTful API documentation with Swagger 2.0. In versions of http-swagger prior to 1.2.6 an attacker may perform a denial of service attack consisting of memory exhaustion on the host system. The cause of the memory exhaustion is down to improper handling of http methods. Users are advised to upgrade. Users unable to upgrade	https://github.com/swaggo/http-swagger/commit/b7d83e8fba85a7a51aa7e45e8244b4173f15049e, https://github.com/swaggo/http-swagger/security/advisories/GHSA-xg75-q3q5-cqmv	A-HTT-HTTP-040522/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may to restrict the path prefix to the "GET" method as a workaround. **CVE ID : CVE-2022-24863**		
Vendor: IBM					
Product: maximo_asset_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Apr-22	5.4	IBM Maximo Asset Management 7.6.1.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. **CVE ID : CVE-2022-22435**	https://www.ibm.com/support/pages/node/6573669, https://exchange.xforce.ibmcloud.com/vulnerabilities/224162	A-IBM-MAXI-040522/122
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Apr-22	5.4	IBM Maximo Asset Management 7.6.1.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 224164.	https://www.ibm.com/support/pages/node/6573667, https://exchange.xforce.ibmcloud.com/vulnerabilities/224164	A-IBM-MAXI-040522/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22436		
Vendor: incsub					
Product: hummingbird					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-22	4.8	The Hummingbird WordPress plugin before 3.3.2 does not sanitise and escape the Config Name, which could allow high privilege users, such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2022-0994**	N/A	A-INC-HUMM-040522/124
Vendor: invicti					
Product: acunetix					
Improper Neutralization of Formula Elements in a CSV File	19-Apr-22	8.8	Invicti Acunetix before 14 allows CSV injection via the Description field on the Add Targets page, if the Export CSV feature is used. **CVE ID : CVE-2022-29315**	N/A	A-INV-ACUN-040522/125
Vendor: jfinalcms_project					
Product: jfinalcms					
Improper Neutralization of Special Elements used in an SQL Command	22-Apr-22	9.8	JFinalCMS v2.0 was discovered to contain a SQL injection vulnerability via the Article Management function.	N/A	A-JFI-JFIN-040522/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2022-27341**		
Vendor: Kentico					
Product: kentico					
Authorization Bypass Through User-Controlled Key	16-Apr-22	4.9	Kentico CMS before 13.0.66 has an Insecure Direct Object Reference vulnerability. It allows an attacker with user management rights (default is Administrator) to export the user options of any user, even ones with higher privileges (like Global Administrators) than the current user. The exported XML contains every option of the exported user (even the hashed password). **CVE ID : CVE-2022-29287**	https://devnet.kentico.com/download/hotfixes	A-KEN-KENT-040522/127
Vendor: Kubernetes					
Product: cri-o					
Incorrect Default Permissions	18-Apr-22	5.3	A flaw was found in cri-o, where containers were incorrectly started with non-empty default permissions. A vulnerability was found in Moby (Docker Engine) where containers started incorrectly	N/A	A-KUB-CRI--040522/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. **CVE ID : CVE-2022-27652**		
Vendor: Liferay					
Product: digital_experience_platform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Apr-22	5.4	Cross-site scripting (XSS) vulnerability in the Asset module's asset categories selector in Liferay Portal 7.3.3 through 7.4.0, and Liferay DXP 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML via the name of a asset category. **CVE ID : CVE-2022-26593**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-26593-stored-xss-with-category-name-in-asset-categories-selector	A-LIF-DIGI-040522/129
Incorrect Default Permissions	19-Apr-22	4.3	Liferay Portal 7.3.7, 7.4.0, and 7.4.1, and Liferay DXP 7.2 fix pack 13, and 7.3 fix pack 2 does not properly check user permission when accessing a list of sites/groups, which	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publishe	A-LIF-DIGI-040522/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows remote authenticated users to view sites/groups via the user's site membership assignment UI. **CVE ID : CVE-2022-26595**	r/HbL5mxmVrnXW/content/cve-2022-26595-unauthorized-access-to-site-group-list	
Product: liferay_portal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Apr-22	5.4	Cross-site scripting (XSS) vulnerability in the Asset module's asset categories selector in Liferay Portal 7.3.3 through 7.4.0, and Liferay DXP 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML via the name of a asset category. **CVE ID : CVE-2022-26593**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-26593-stored-xss-with-category-name-in-asset-categories-selector	A-LIF-LIFE-040522/131
Incorrect Default Permissions	19-Apr-22	4.3	Liferay Portal 7.3.7, 7.4.0, and 7.4.1, and Liferay DXP 7.2 fix pack 13, and 7.3 fix pack 2 does not properly check user permission when accessing a list of sites/groups, which allows remote authenticated users to view sites/groups via the user's site membership assignment UI.	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-26595-unauthorized-access-to-site-group-list	A-LIF-LIFE-040522/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26595		
Vendor: link-admin_project					
Product: link-admin					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Apr-22	9.8	Link-Admin v0.0.1 was discovered to contain a SQL injection vulnerability via DictRest.ResponseResult(). **CVE ID : CVE-2022-27342**	N/A	A-LIN-LINK-040522/133
Vendor: loco_translate_project					
Product: loco_translate					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-22	5.4	The Loco Translate WordPress plugin before 2.6.1 does not properly remove inline events from elements in the source translation strings before outputting them in the editor in the plugin admin panel, allowing any user with access to the plugin (Translator and Administrator by default) to add arbitrary javascript payloads to the source strings leading to a stored cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2022-0765**	N/A	A-LOC-LOCO-040522/134
Vendor: mattermost					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mattermost_server					
Missing Authorization	19-Apr-22	8.8	Mattermost version 6.4.x and earlier fails to properly check the plugin version when a plugin is installed from the Marketplace, which allows an authenticated and an authorized user to install and exploit an old plugin version from the Marketplace which might have known vulnerabilities. **CVE ID : CVE-2022-1384**	https://mattermost.com/security-updates/	A-MAT-MATT-040522/135
Exposure of Resource to Wrong Sphere	19-Apr-22	4.6	Mattermost 6.4.x and earlier fails to properly invalidate pending email invitations when the action is performed from the system console, which allows accidentally invited users to join the workspace and access information from the public teams and channels. **CVE ID : CVE-2022-1385**	https://mattermost.com/security-updates/	A-MAT-MATT-040522/136
Vendor: Mcafee					
Product: web_gateway					
URL Redirection to Untrusted	20-Apr-22	6.1	A URL redirection vulnerability in Skyhigh SWG in main releases 10.x prior to 10.2.9, 9.x prior to	https://kc.mcafee.com/corporate/index?page=	A-MCA-WEB_-040522/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			9.2.20, 8.x prior to 8.2.27, and 7.x prior to 7.8.2.31, and controlled release 11.x prior to 11.1.3 allows a remote attacker to redirect a user to a malicious website controlled by the attacker. This is possible because SWG incorrectly creates a HTTP redirect response when a user clicks a carefully constructed URL. Following the redirect response, the new request is still filtered by the SWG policy. **CVE ID : CVE-2022-1254**	content&id=SB10381	
Vendor: microfinance_management_system_project					
Product: microfinance_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Apr-22	9.8	A SQL injection vulnerability exists in Microfinance Management System 1.0 when MySQL is being used as the application database. An attacker can issue SQL commands to the MySQL database through the vulnerable course_code and/or customer_number parameter. **CVE ID : CVE-2022-27927**	N/A	A-MIC-MICR-040522/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Microweber					
Product: microweber					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-22	6.1	Reflected XSS on demo.microweber.org/demo/module/ in GitHub repository microweber/microweber prior to 1.2.15. Execute Arbitrary JavaScript as the attacked user. It's the only payload I found working, you might need to press "tab" but there is probably a paylaod that runs without user interaction. **CVE ID : CVE-2022-1439**	https://huntr.dev/bounties/86f6a762-0f3d-443d-a676-20f8496907e0, https://github.com/microweber/microweber/commit/ad3928f67b2cd4443f4323d858b666d35a919ba8	A-MIC-MICR-040522/139
Vendor: Misp					
Product: misp					
Deserialization of Untrusted Data	20-Apr-22	9.8	An issue was discovered in MISP before 2.4.158. PHAR deserialization can occur. **CVE ID : CVE-2022-29528**	https://github.com/MISP/MISP/commit/0108f1bde2117ac5c1e28d124128f60c8bb09a8e, https://github.com/MISP/MISP/commit/93821c0de6a7dd32262ce62212773f43136ca66e	A-MIS-MISP-040522/140
Improper Neutralization of Input During Web Page Generation	20-Apr-22	5.4	An issue was discovered in MISP before 2.4.158. There is stored XSS via the LinOTP login field. **CVE ID : CVE-2022-29529**	https://github.com/MISP/MISP/commit/9623de2f5cca011afc581d55cfa5ce87682894fd	A-MIS-MISP-040522/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-22	5.4	An issue was discovered in MISP before 2.4.158. There is stored XSS in the galaxy clusters. **CVE ID : CVE-2022-29530**	https://github.com/MISP/MISP/commit/107e271d78c255d658ce998285fe6f6c4f291b41	A-MIS-MISP-040522/142
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-22	5.4	An issue was discovered in MISP before 2.4.158. There is stored XSS in the event graph via a tag name. **CVE ID : CVE-2022-29531**	https://github.com/MISP/MISP/commit/bb3b7a7e91862742cae228c43b3091bad476dcc0	A-MIS-MISP-040522/143
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-22	4.8	An issue was discovered in MISP before 2.4.158. There is XSS in the cerebrate view if one administrator puts a javascript: URL in the URL field, and another administrator clicks on it. **CVE ID : CVE-2022-29532**	https://github.com/MISP/MISP/commit/60c85b80e3ab05c3ef015bca5630e95eddbb1436	A-MIS-MISP-040522/144
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-22	6.1	An issue was discovered in MISP before 2.4.158. There is XSS in app/Controller/OrganisationsController.php in a situation with a "weird single checkbox page."	https://github.com/MISP/MISP/commit/ce6bc88e330f5ef50666b149d86c0d94f545f24e	A-MIS-MISP-040522/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29533		
Improper Authentication	20-Apr-22	7.5	An issue was discovered in MISP before 2.4.158. In UsersController.php, password confirmation can be bypassed via vectors involving an "Accept: application/json" header. **CVE ID : CVE-2022-29534**	https://github.com/MISP/MISP/commit/01120163a6b4d905029d416e7305575df31df8af	A-MIS-MISP-040522/146
Vendor: mobyproject					
Product: moby					
Incorrect Default Permissions	18-Apr-22	5.3	A flaw was found in cri-o, where containers were incorrectly started with non-empty default permissions. A vulnerability was found in Moby (Docker Engine) where containers started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. **CVE ID : CVE-2022-27652**	N/A	A-MOB-MOBY-040522/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: nextauth.js					
Product: next-auth					
URL Redirection to Untrusted Site ('Open Redirect')	19-Apr-22	6.1	next-auth v3 users before version 3.29.2 are impacted. next-auth version 4 users before version 4.3.2 are also impacted. Upgrading to 3.29.2 or 4.3.2 will patch this vulnerability. If you are not able to upgrade for any reason, you can add a configuration to your callbacks option. If you already have a `redirect` callback, make sure that you match the incoming `url` origin against the `baseUrl`. **CVE ID : CVE-2022-24858**	https://next-auth.js.org/getting-started/upgrade-v4, https://next-auth.js.org/configuration/callbacks#redirect-callback, https://github.com/nextauthjs/next-auth/security/advisories/GHSA-f9wg-5f46-cjmw	A-NEX-NEXT-040522/148
Vendor: Oracle					
Product: agile_plm					
N/A	19-Apr-22	6.5	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Attachments). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM.	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-AGIL-040522/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile PLM accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21467**		
Product: banking_payments					
Incorrect Permission Assignment for Critical Resource	19-Apr-22	5.9	Vulnerability in the Oracle Banking Payments product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-BANK-040522/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			creation, deletion or modification access to critical data or all Oracle Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Payments. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:L). **CVE ID : CVE-2022-21475**		
Product: business_intelligence					
N/A	19-Apr-22	6.1	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.5.0.0.0 and 5.9.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-BUSI-040522/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21419		
N/A	19-Apr-22	7.5	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 5.5.0.0.0, 5.9.0.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21421**	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-BUSI-040522/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-22	6.1	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Server). The supported version that is affected is 5.9.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-BUSI-040522/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21492**		
Product: coherence					
N/A	19-Apr-22	9.8	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-COHE-040522/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21420**		
Product: commerce_guided_search					
N/A	19-Apr-22	7.5	Vulnerability in the Oracle Commerce Guided Search product of Oracle Commerce (component: Tools and Frameworks). The supported version that is affected is 11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21466**	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-COMM-040522/155
Product: communications_billing_and_revenue_management					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-22	7.5	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.4 and 12.0.0.5. Difficult to exploit vulnerability allows low privileged attacker with network access via TCP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21422**	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-COMM-040522/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-22	8.3	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). The supported version that is affected is 12.0.0.4. Easily exploitable vulnerability allows low privileged attacker with network access via TCP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Communications Billing and Revenue Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Communications Billing and Revenue Management accessible data and	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-COMM-040522/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L). **CVE ID : CVE-2022-21424**		
N/A	19-Apr-22	8.5	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.4 and 12.0.0.5. Difficult to exploit vulnerability allows low privileged attacker with network access via TCP to compromise Oracle Communications Billing and Revenue Management. While the vulnerability is in	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-COMM-040522/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Communications Billing and Revenue Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-21430**		
N/A	19-Apr-22	10	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.4 and 12.0.0.5. Easily exploitable vulnerability allows unauthenticated attacker with	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-COMM-040522/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network access via TCP to compromise Oracle Communications Billing and Revenue Management. While the vulnerability is in Oracle Communications Billing and Revenue Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-21431**		
Product: database					
N/A	19-Apr-22	7.2	Vulnerability in the Oracle Database - Enterprise Edition Sharding component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-DATA-040522/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			high privileged attacker having Create Any Procedure privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Sharding. Successful attacks of this vulnerability can result in takeover of Oracle Database - Enterprise Edition Sharding. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21410**		
N/A	19-Apr-22	5.4	Vulnerability in the RDBMS Gateway / Generic ODBC Connectivity component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-DATA-040522/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise RDBMS Gateway / Generic ODBC Connectivity. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of RDBMS Gateway / Generic ODBC Connectivity accessible data as well as unauthorized read access to a subset of RDBMS Gateway / Generic ODBC Connectivity accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2022-21411**		
N/A	19-Apr-22	6.5	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Procedure privilege with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-DATA-040522/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2022-21498**		
Product: goldengate					
N/A	19-Apr-22	8.8	Vulnerability in Oracle GoldenGate (component: OGG Core Library). The supported version that is affected is Prior to 23.1. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle GoldenGate executes to compromise Oracle GoldenGate. While the vulnerability is in Oracle GoldenGate, attacks may significantly impact additional products (scope change). Successful attacks of	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-GOLD-040522/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in takeover of Oracle GoldenGate. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-21442**		
Product: graalvm					
N/A	19-Apr-22	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0006/	A-ORA-GRAA-040522/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21426**		
N/A	19-Apr-22	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component:	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security	A-ORA-GRAA-040522/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability	.netapp.com/advisory/ntap-20220429-0006/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21434**		
N/A	19-Apr-22	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0006/	A-ORA-GRAA-040522/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21443**		
N/A	19-Apr-22	7.5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle	https://www.oracle.com/security-alerts/cpuapr2022.html,	A-ORA-GRAA-040522/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 17.0.2 and 18; Oracle GraalVM Enterprise Edition: 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability	https://security.netapp.com/advisory/ntap-20220429-0006/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2022-21449**		
N/A	19-Apr-22	7.5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0006/	A-ORA-GRAA-040522/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21476**		
N/A	19-Apr-22	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle	https://www.oracle.com/security-alerts/cpuapr2022.html,	A-ORA-GRAA-040522/169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.	https://security.netapp.com/advisory/ntap-20220429-0006/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21496**		
Product: helidon					
N/A	19-Apr-22	8.1	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Reactive WebServer). Supported versions that are affected are 1.4.10 and 2.0.0-RC1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in takeover of Helidon. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-HELI-040522/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21404**		
Product: java_se					
N/A	19-Apr-22	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments,	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0006/	A-ORA-JAVA-040522/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21434**		
N/A	19-Apr-22	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Difficult to exploit	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0006/	A-ORA-JAVA-040522/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21443**		
Product: jdeveloper					
N/A	19-Apr-22	9.8	Vulnerability in the Oracle JDeveloper product of Oracle Fusion Middleware (component: ADF Faces). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle JDeveloper. Successful attacks of this vulnerability can result in takeover of Oracle JDeveloper. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21445**	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-JDEV-040522/173
Product: jdk					
N/A	19-Apr-22	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM	https://www.oracle.com/security-	A-ORA-JDK-040522/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet)	alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0006/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21426**		
N/A	19-Apr-22	7.5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 17.0.2 and 18; Oracle GraalVM Enterprise Edition: 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0006/	A-ORA-JDK-040522/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2022-21449**		
N/A	19-Apr-22	7.5	Vulnerability in the Oracle Java SE, Oracle GraalVM	https://www.oracle.com/security-	A-ORA-JDK-040522/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet)	alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0006/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21476**		
N/A	19-Apr-22	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0006/	A-ORA-JDK-040522/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21496**		
Product: jd_edwards_enterpriseone_tools					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-22	6.1	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime). The supported version that is affected is Prior to 9.2.6.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-JD_E-040522/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21409**		
N/A	19-Apr-22	8.2	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Business Logic Infra SEC). The supported version that is affected is Prior to 9.2.6.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of JD Edwards EnterpriseOne Tools and unauthorized read access to a subset of JD Edwards EnterpriseOne Tools	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-JD_E-040522/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H). **CVE ID : CVE-2022-21464**		
Product: jre					
N/A	19-Apr-22	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0006/	A-ORA-JRE-040522/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21426**		
Product: mysql					
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior.	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-	A-ORA-MYSQ-040522/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21412**	20220429-0005/	
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21417**		
N/A	19-Apr-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21425**		
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21427**		
N/A	19-Apr-22	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21444**	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-22	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21454**	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/186
N/A	19-Apr-22	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/ad	A-ORA-MYSQ-040522/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.7.37 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21460**	visory/ntap-20220429-0005/	
N/A	19-Apr-22	6.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21489**		
Product: mysql_cluster					
N/A	19-Apr-22	6.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21490**		
Product: mysql_server					
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21413**		
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21414**		
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21415**	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-22	5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21418**	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/193
N/A	19-Apr-22	2.7	Vulnerability in the MySQL Server product of Oracle MySQL (component:	https://www.oracle.com/security-alerts/cpuapr2	A-ORA-MYSQ-040522/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InnoDB). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21423**	022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21435**		
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21436**		
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21437		
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21438**	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/198
N/A	19-Apr-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/ad	A-ORA-MYSQ-040522/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21440**	visory/ntap-20220429-0005/	
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21452**		
N/A	19-Apr-22	5.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PAM Auth Plugin). Supported versions that are affected are 8.0.28 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21457**		
N/A	19-Apr-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21459**		
N/A	19-Apr-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuapr2022.html, https://security.netapp.com/advisory/ntap-20220429-0005/	A-ORA-MYSQ-040522/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21462		
Product: oss_support_tools					
N/A	19-Apr-22	5.5	Vulnerability in the OSS Support Tools product of Oracle Support Tools (component: Oracle Explorer). The supported version that is affected is 18.3. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where OSS Support Tools executes to compromise OSS Support Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in OSS Support Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all OSS Support Tools accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-OSS_-040522/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2022-21405**		
Product: peoplesoft_enterprise_peopletools					
N/A	19-Apr-22	6.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Navigation Pages, Portal, Query). Supported versions that are affected are 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-PEOP-040522/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21456**		
N/A	19-Apr-22	6.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Navigation Pages, Portal, Query). Supported versions that are affected are 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-PEOP-040522/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21458**		
Product: vm_virtualbox					
N/A	19-Apr-22	6.7	Vulnerability in the Oracle VM VirtualBox	https://www.oracle.com/securi	A-ORA-VM_V-040522/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.34. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.7 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L	ty-alerts/cpuapr2022.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:H/UI:N/S:C/C:N/I:L/A:H). **CVE ID : CVE-2022-21465**		
N/A	19-Apr-22	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.34. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-VM_V-040522/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:L/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2022-21487**		
N/A	19-Apr-22	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.34. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-VM_V-040522/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:L/UI:N/S:C/C:N/I:L/A:N). **CVE ID : CVE-2022-21488**		
N/A	19-Apr-22	7.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.34. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21491**	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-VM_V-040522/210
Product: weblogic_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-22	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3/IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21441**	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-WEBL-040522/211
Product: web_services_manager					
N/A	19-Apr-22	8.1	Vulnerability in the Oracle Web Services Manager product of Oracle Fusion Middleware	https://www.oracle.com/security-alerts/cpuapr2022.html	A-ORA-WEB_-040522/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: Web Services Security). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Services Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Web Services Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Web Services Manager accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2022-21497**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: originprotocol					
Product: origin_website					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-22	5.4	Origin Protocol is a blockchain based project. The Origin Protocol project website allows for malicious users to inject malicious Javascript via a POST request to `/presale/join`. User-controlled data is passed with no sanitization to SendGrid and injected into an email that is delivered to the founders@originprotocol.com. If the email recipient is using an email program that is susceptible to XSS, then that email recipient will receive an email that may contain malicious XSS. Regardless if the email recipient's mail program has vulnerabilities or not, the hacker can at the very least inject malicious HTML that modifies the body content of the email. There are currently no known workarounds. **CVE ID : CVE-2022-24864**	https://github.com/OriginProtocol/origin-website/pull/617, https://github.com/github/codeql/pull/7127, https://github.com/OriginProtocol/origin-website/security/advisories/GHSA-v6fc-qwxx-m4h7	A-ORI-ORIG-040522/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Pimcore					
Product: pimcore					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Apr-22	7.5	SQL injection in GridHelperService.php in GitHub repository pimcore/pimcore prior to 10.3.6. This vulnerability is capable of steal the data **CVE ID : CVE-2022-1429**	https://github.com/pimcore/pimcore/commit/523a735ab94f004459b84ffdfd3db784586bbd82, https://huntr.dev/bounties/cfba30b4-85fa-4499-9160-cd6e3119310e	A-PIM-PIMC-040522/214
Vendor: posthog					
Product: posthog					
URL Redirection to Untrusted Site ('Open Redirect')	19-Apr-22	6.1	Open redirect vulnerability via endpoint authorize_and_redirect/?redirect= in GitHub repository posthog/posthog prior to 1.34.1. **CVE ID : CVE-2022-0645**	https://huntr.dev/bounties/c13258a2-30e3-4261-9a3b-2f39c49a8bd6, https://github.com/posthog/posthog/commit/859d8ed9ac7c5026db09714a26c85c1458abb038	A-POS-POST-040522/215
Vendor: purchase_order_management_system_project					
Product: purchase_order_management_system					
Unrestricted Upload of File with Dangerous Type	21-Apr-22	9.8	Purchase Order Management System v1.0 was discovered to contain a remote code execution (RCE) vulnerability via /purchase_order/admin/?page=user. **CVE ID : CVE-2022-28021**	N/A	A-PUR-PURC-040522/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Purchase Order Management System v1.0 was discovered to contain a SQL injection vulnerability via /purchase_order/classes/Master.php?f=delete_item. **CVE ID : CVE-2022-28022**	N/A	A-PUR-PURC-040522/217
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Purchase Order Management System v1.0 was discovered to contain a SQL injection vulnerability via /purchase_order/classes/Master.php?f=delete_supplier. **CVE ID : CVE-2022-28023**	N/A	A-PUR-PURC-040522/218
Vendor: pypdf2_project					
Product: pypdf2					
Loop with Unreachable Exit Condition ('Infinite Loop')	18-Apr-22	5.5	PyPDF2 is an open source python PDF library capable of splitting, merging, cropping, and transforming the pages of PDF files. In versions prior to 1.27.5 an attacker who uses this vulnerability can craft a PDF which leads to an infinite loop if the PyPDF2 if the code attempts to get the content stream. The reason is that the last while-	https://github.com/py-pdf/PyPDF2/security/advisories/GHSA-xcjx-m2pj-8g79, https://github.com/py-pdf/PyPDF2/pull/740	A-PYP-PYPD-040522/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			loop in `ContentStream._readInlineImage` only terminates when it finds the `EI` token, but never actually checks if the stream has already ended. This issue has been resolved in version `1.27.5`. Users unable to upgrade should validate and PDFs prior to iterating over their content stream. **CVE ID : CVE-2022-24859**		
Vendor: Radare					
Product: radare2					
NULL Pointer Dereference	18-Apr-22	5.5	NULL Pointer Dereference in GitHub repository radareorg/radare2 prior to 5.6.8. This vulnerability is capable of making the radare2 crash, thus affecting the availability of the system. **CVE ID : CVE-2022-1382**	https://github.com/radareorg/radare2/commit/48f0ea79f99174fb0a62cb2354e13496ce5b7c44, https://huntr.dev/bounties/d8b6d239-6d7b-4783-b26b-5be848c01aa1	A-RAD-RADA-040522/220
Out-of-bounds Write	18-Apr-22	6.1	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.6.8. The bug causes the program reads data past the end of the intented buffer.	https://huntr.dev/bounties/02b4b563-b946-4343-9092-38d1c5cd60c9, https://github.com/radareorg/radare2/commit/1dd65336f0f0	A-RAD-RADA-040522/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash. **CVE ID : CVE-2022-1383**	c351d6ea853efcf73cf9c0030862	
Vendor: Redhat					
Product: openshift_container_platform					
Incorrect Default Permissions	18-Apr-22	5.3	A flaw was found in cri-o, where containers were incorrectly started with non-empty default permissions. A vulnerability was found in Moby (Docker Engine) where containers started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. **CVE ID : CVE-2022-27652**	N/A	A-RED-OPEN-040522/222
Vendor: sandhillsdev					
Product: easy_digital_downloads					
Improper Neutralization of Input	18-Apr-22	4.8	The Easy Digital Downloads WordPress plugin	https://wpscan.com/vulnerability/598d5c1b-	A-SAN-EASY-040522/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			before 2.11.6 does not sanitise and escape the Downloadable File Name in the Logs, which could allow high privilege users to perform Cross-Site Scripting attacks when the unfiltered_html capability is disallowed **CVE ID : CVE-2022-0706**	7930-46a6-9a31-5e08a5f14907, https://plugins.trac.wordpress.org/changeset/2697388	
Cross-Site Request Forgery (CSRF)	18-Apr-22	4.3	The Easy Digital Downloads WordPress plugin before 2.11.6 does not have CSRF check in place when inserting payment notes, which could allow attackers to make a logged admin insert arbitrary notes via a CSRF attack **CVE ID : CVE-2022-0707**	https://plugins.trac.wordpress.org/changeset/2697388, https://wpscan.com/vulnerability/50680797-61e4-4737-898f-e5b394d89117	A-SAN-EASY-040522/224
Vendor: searchiq					
Product: searchiq					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-22	6.1	The SearchIQ WordPress plugin before 3.9 contains a flag to disable the verification of CSRF nonces, granting unauthenticated attackers access to the siq_ajax AJAX action and allowing them to perform	N/A	A-SEA-SEAR-040522/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cross-Site Scripting attacks due to the lack of sanitisation and escaping in the customCss parameter **CVE ID : CVE-2022-0780**		
Vendor: selenium					
Product: selenium_grid					
Cross-Site Request Forgery (CSRF)	19-Apr-22	8.8	Selenium Server (Grid) before 4 allows CSRF because it permits non-JSON content types such as application/x-www-form-urlencoded, multipart/form-data, and text/plain. **CVE ID : CVE-2022-28108**	https://www.selenium.dev/downloads/	A-SEL-SELE-040522/226
Vendor: Shopware					
Product: shopware					
Server-Side Request Forgery (SSRF)	20-Apr-22	5.5	Shopware is an open commerce platform based on Symfony Framework and Vue. In affected versions an attacker can abuse the Admin SDK functionality on the server to read or update internal resources. Users are advised to update to the current version 6.4.10.1. For older versions of 6.1, 6.2, and 6.3, corresponding security measures	https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-04-2022, https://github.com/shopware/platform/commit/083765e2d64a00315050c4891800c9e98ba0c77c, https://github.com/shopware/platform/security/advisories/G	A-SHO-SHOP-040522/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are also available via a plugin. There are no known workarounds for this issue. **CVE ID : CVE-2022-24871**	HSA-7gm7-8q8v-9gf2	
Vendor: simplefilelist					
Product: simple-file-list					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Apr-22	7.5	The Simple File List WordPress plugin is vulnerable to Arbitrary File Download via the eeFile parameter found in the ~/includes/ee-downloader.php file due to missing controls which makes it possible unauthenticated attackers to supply a path to a file that will subsequently be downloaded, in versions up to and including 3.2.7. **CVE ID : CVE-2022-1119**	https://plugins.trac.wordpress.org/browser/simple-file-list/trunk/includes/ee-downloader.php?rev=2071880	A-SIM-SIMP-040522/228
Vendor: simple_real_estate_portal_system_portal					
Product: simple_real_estate_portal_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection vulnerability via /reps/admin/?page=agents/manage_agent.	N/A	A-SIM-SIMP-040522/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28411		
Vendor: simple_real_estate_portal_system_project					
Product: simple_real_estate_portal_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection vulnerability via /reps/classes/Master.php?f=delete_amenity. **CVE ID : CVE-2022-28028**	N/A	A-SIM-SIMP-040522/230
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection vulnerability via /reps/classes/Master.php?f=delete_type. **CVE ID : CVE-2022-28029**	N/A	A-SIM-SIMP-040522/231
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection vulnerability via /reps/classes/Master.php?f=delete_estate. **CVE ID : CVE-2022-28030**	N/A	A-SIM-SIMP-040522/232
Improper Neutralization of Special Elements used in an	21-Apr-22	9.8	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection	N/A	A-SIM-SIMP-040522/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			vulnerability via /reps/classes/Users.php?f=delete_agent. **CVE ID : CVE-2022-28410**		
Vendor: siteground					
Product: siteground_security					
Improper Authentication	19-Apr-22	9.8	The SiteGround Security plugin for WordPress is vulnerable to authentication bypass that allows unauthenticated users to log in as administrative users due to missing identity verification on initial 2FA set-up that allows unauthenticated and unauthorized users to configure 2FA for pending accounts. Upon successful configuration, the attacker is logged in as that user without access to a username/password pair which is the expected first form of authentication. This affects versions up to, and including, 1.2.5. **CVE ID : CVE-2022-0992**	https://plugins.trac.wordpress.org/changeset/2706302	A-SIT-SITE-040522/234
Improper Authentication	19-Apr-22	9.8	The SiteGround Security plugin for WordPress is vulnerable to	https://plugins.trac.wordpress.org/changeset/2706302	A-SIT-SITE-040522/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication bypass that allows unauthenticated users to log in as administrative users due to missing identity verification on the 2FA back-up code implementation that logs users in upon success. This affects versions up to, and including, 1.2.5. **CVE ID : CVE-2022-0993**		
Vendor: snipeitapp					
Product: snipe-it					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Apr-22	5.4	Stored Cross Site Scripting vulnerability in Item name parameter in GitHub repository snipe/snipe-it prior to v5.4.3. The vulnerability is capable of stolen the user Cookie. **CVE ID : CVE-2022-1380**	https://huntr.dev/bounties/3d45cfca-3a72-4578-b735-98837b998a12, https://github.com/snipe/snipe-it/commit/f211c11034baf4281aa62e7b5e0347248d995ee9	A-SNI-SNIP-040522/236
Vendor: stripe					
Product: smokescreen					
Server-Side Request Forgery (SSRF)	19-Apr-22	5.3	Smokescreen is a simple HTTP proxy that fogs over naughty URLs. The primary use case for Smokescreen is to prevent server-side request forgery (SSRF) attacks in	https://github.com/stripe/smokescreen/security/advisories/GHSA-gcj7-j438-hjj2	A-STR-SMOK-040522/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which external attackers leverage the behavior of applications to connect to or scan internal infrastructure. Smokescreen also offers an option to deny access to additional (e.g., external) URLs by way of a deny list. There was an issue in Smokescreen that made it possible to bypass the deny list feature by appending a dot to the end of user-supplied URLs, or by providing input in a different letter case. Recommended to upgrade Smokescreen to version 0.0.3 or later. **CVE ID : CVE-2022-24825**		
Vendor: student_grading_system_project					
Product: student_grading_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Student Grading System v1.0 was discovered to contain a SQL injection vulnerability via /student-grading-system/rms.php?page=grade. **CVE ID : CVE-2022-28024**	N/A	A-STU-STUD-040522/238
Improper Neutralizatio	21-Apr-22	9.8	Student Grading System v1.0 was	N/A	A-STU-STUD-040522/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			discovered to contain a SQL injection vulnerability via /student-grading-system/rms.php?page=school_year. **CVE ID : CVE-2022-28025**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-22	9.8	Student Grading System v1.0 was discovered to contain a SQL injection vulnerability via /student-grading-system/rms.php?page=student_p&id=. **CVE ID : CVE-2022-28026**	N/A	A-STU-STUD-040522/240
Vendor: text_hover_project					
Product: text_hover					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-22	4.8	The Text Hover WordPress plugin before 4.2 does not sanitize and escape the text to hover, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-0737**	N/A	A-TEX-TEXT-040522/241
Vendor: thank_me_later_project					
Product: thank_me_later					
Improper Neutralization of Input During Web	18-Apr-22	4.8	The Thank Me Later WordPress plugin through 3.3.4 does not sanitise and	N/A	A-THA-THAN-040522/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			escape the Message Subject field before outputting it in the Messages list, which could allow high privileges users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2022-1063**		
Vendor: Tylertech					
Product: odyssey					
Authorization Bypass Through User-Controlled Key	18-Apr-22	7.5	An Insecure Direct Object Reference issue exists in the Tyler Odyssey platform before 17.1.20. This may allow an external party to access sensitive case records. **CVE ID : CVE-2022-26665**	https://www.tylertech.com/dataharvest	A-TYL-ODYS-040522/243
Vendor: victor_cms_project					
Product: victor_cms					
Unrestricted Upload of File with Dangerous Type	21-Apr-22	8.8	Victor v1.0 was discovered to contain a remote code execution (RCE) vulnerability via the component admin/profile.php?section=admin. **CVE ID : CVE-2022-27478**	N/A	A-VIC-VICT-040522/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Videowhisper					
Product: micropayments					
Cross-Site Request Forgery (CSRF)	20-Apr-22	8.8	Cross-site request forgery (CSRF) vulnerability in 'MicroPayments - Paid Author Subscriptions, Content, Downloads, Membership' versions prior to 1.9.6 allows a remote unauthenticated attacker to hijack the authentication of an administrator and perform unintended operation via unspecified vectors. **CVE ID : CVE-2022-27629**	https://plugins.trac.wordpress.org/changeset?new=2362275%40paid-membership&old=2345274%40paid-membership	A-VID-MICR-040522/245
Vendor: vikwp					
Product: vikbooking_hotel_booking_engine_\&_property_management_system_plugin					
Unrestricted Upload of File with Dangerous Type	19-Apr-22	9.8	Arbitrary File Upload leading to RCE in E4J s.r.l. VikBooking Hotel Booking Engine & PMS plugin <= 1.5.3 on WordPress allows attackers to upload and execute dangerous file types (e.g. PHP shell) via the signature upload on the booking form. **CVE ID : CVE-2022-27862**	https://wordpress.org/plugins/vikbooking/#developers, https://patchstack.com/database/vulnerability/vikbooking/wordpress-vikbooking-hotel-booking-engine-pms-plugin-1-5-3-arbitrary-file-upload-leading-to-rce	A-VIK-VIKB-040522/246
Exposure of Sensitive Information	19-Apr-22	5.3	Sensitive Information Exposure in E4J s.r.l.	https://patchstack.com/database/vulnerability	A-VIK-VIKB-040522/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to an Unauthorized Actor			VikBooking Hotel Booking Engine & PMS plugin <= 1.5.3 on WordPress allows attackers to get the booking data by guessing / brute-forcing easy predictable booking IDs via search POST requests. **CVE ID : CVE-2022-27863**	/vikbooking/wordpress-vikbooking-hotel-booking-engine-pms-plugin-1-5-3-sensitive-data-exposure-vulnerability, https://wordpress.org/plugins/vikbooking/#developers	
Vendor: villatheme					
Product: exmage					
Server-Side Request Forgery (SSRF)	18-Apr-22	7.2	The EXMAGE WordPress plugin before 1.0.7 does to ensure that images added via URLs are external images, which could lead to a blind SSRF issue by using local URLs **CVE ID : CVE-2022-1037**	N/A	A-VIL-EXMA-040522/248
Vendor: VIM					
Product: vim					
Out-of-bounds Write	18-Apr-22	7.8	global heap buffer overflow in skip_range in GitHub repository vim/vim prior to 8.2.4763. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution	https://huntr.dev/bounties/55f9c0e8-c221-48b6-a00e-bdcaebaba4a4, https://github.com/vim/vim/commit/f50808ed135ab973296bca515ae4029b321afe47	A-VIM-VIM-040522/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1381		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Apr-22	5.5	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4774. **CVE ID : CVE-2022-1420**	https://github.com/vim/vim/commit/8b91e71441069b1dde9ac9ff9d9a829b1b4aecca, https://huntr.dev/bounties/a4323ef8-90ea-4e1c-90e9-c778f0ecf326	A-VIM-VIM-040522/250
Vendor: wasm3_project					
Product: wasm3					
Out-of-bounds Write	16-Apr-22	5.5	Wasm3 0.5.0 has a heap-based buffer overflow in NewCodePage in m3_code.c (called indirectly from Compile_BranchTable in m3_compile.c). **CVE ID : CVE-2022-28966**	N/A	A-WAS-WASM-040522/251
Vendor: web-x.co					
Product: be_popia_compliant					
Exposure of Sensitive Information to an Unauthorized Actor	19-Apr-22	5.3	The WordPress plugin Be POPIA Compliant exposed sensitive information to unauthenticated users consisting of site visitors emails and usernames via an API route, in versions up to an including 1.1.5. **CVE ID : CVE-2022-1186**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2701343%40be-popia-compliant&new=2701343%40be-popia-compliant&sfp_email=&sfph_mail=	A-WEB-BE_P-040522/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wpchill					
Product: rsvp_and_event_management					
Missing Authorization	18-Apr-22	5.3	The RSVP and Event Management Plugin WordPress plugin before 2.7.8 does not have any authorisation checks when exporting its entries, and has the export function hooked to the init action. As a result, unauthenticated attackers could call it and retrieve PII such as first name, last name and email address of user registered for events **CVE ID : CVE-2022-1054**	N/A	A-WPC-RSVP-040522/253
Vendor: wp_downgrade_project					
Product: wp_downgrade					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-22	4.8	The WP Downgrade WordPress plugin before 1.2.3 only perform client side validation of its "WordPress Target Version" settings, but does not sanitise and escape it server side, allowing high privilege users such as admin to perform Cross-Site attacks even when the unfiltered_html capability is disallowed	https://wpscan.com/vulnerability/34a7b3cd-e2b5-4891-ab33-af6a2a0eeceb, https://plugins.trac.wordpress.org/changeset/2696091	A-WP_-WP_D-040522/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1001		
Vendor: wp_youtube_live_project					
Product: wp_youtube_live					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Apr-22	6.1	The WordPress WP YouTube Live Plugin is vulnerable to Reflected Cross-Site Scripting via POST data found in the ~/inc/admin.php file which allows unauthenticated attackers to inject arbitrary web scripts in versions up to, and including, 1.7.21. **CVE ID : CVE-2022-1187**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2702715%40wp-youtube-live&new=2702715%40wp-youtube-live&sfp_email=&sfph_mail=	A-WP_-WP_Y-040522/255
Vendor: Wso2					
Product: api_manager					
Unrestricted Upload of File with Dangerous Type	18-Apr-22	9.8	Certain WSO2 products allow unrestricted file upload with resultant remote code execution. The attacker must use a /fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a ../../../../repository/deployment/server/webapps directory. This affects WSO2 API Manager 2.2.0 and above through 4.0.0; WSO2 Identity	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738	A-WSO-API_-040522/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server 5.2.0 and above through 5.11.0; WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0; WSO2 Identity Server as Key Manager 5.3.0 and above through 5.10.0; and WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0. **CVE ID : CVE-2022-29464**		
Product: enterprise_integrator					
Unrestricted Upload of File with Dangerous Type	18-Apr-22	9.8	Certain WSO2 products allow unrestricted file upload with resultant remote code execution. The attacker must use a /fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a ../../../../repository/deployment/server/webapps directory. This affects WSO2 API Manager 2.2.0 and above through 4.0.0; WSO2 Identity Server 5.2.0 and above through 5.11.0; WSO2 Identity Server Analytics 5.4.0, 5.4.1,	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738	A-WSO-ENTE-040522/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.5.0, and 5.6.0; WSO2 Identity Server as Key Manager 5.3.0 and above through 5.10.0; and WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0. **CVE ID : CVE-2022-29464**		
Product: identity_server					
Unrestricted Upload of File with Dangerous Type	18-Apr-22	9.8	Certain WSO2 products allow unrestricted file upload with resultant remote code execution. The attacker must use a /fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a ../../../../repository/deployment/server/webapps directory. This affects WSO2 API Manager 2.2.0 and above through 4.0.0; WSO2 Identity Server 5.2.0 and above through 5.11.0; WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0; WSO2 Identity Server as Key Manager 5.3.0 and above through	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738	A-WSO-IDEN-040522/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.10.0; and WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0. **CVE ID : CVE-2022-29464**		
Product: identity_server_analytics					
Unrestricted Upload of File with Dangerous Type	18-Apr-22	9.8	Certain WSO2 products allow unrestricted file upload with resultant remote code execution. The attacker must use a /fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a ../../../../repository/deployment/server/webapps directory. This affects WSO2 API Manager 2.2.0 and above through 4.0.0; WSO2 Identity Server 5.2.0 and above through 5.11.0; WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0; WSO2 Identity Server as Key Manager 5.3.0 and above through 5.10.0; and WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0.	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738	A-WSO-IDEN-040522/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29464		
Product: identity_server_as_key_manager					
Unrestricted Upload of File with Dangerous Type	18-Apr-22	9.8	Certain WSO2 products allow unrestricted file upload with resultant remote code execution. The attacker must use a /fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a ../../../../repository/deployment/server/webapps directory. This affects WSO2 API Manager 2.2.0 and above through 4.0.0; WSO2 Identity Server 5.2.0 and above through 5.11.0; WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0; WSO2 Identity Server as Key Manager 5.3.0 and above through 5.10.0; and WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0. **CVE ID : CVE-2022-29464**	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738	A-WSO-IDEN-040522/260
Vendor: Zimbra					
Product: collaboration					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Apr-22	6.1	A reflected cross-site scripting (XSS) vulnerability in the /public/launchNewWindow.jsp component of Zimbra Collaboration (aka ZCS) 9.0 allows unauthenticated attackers to execute arbitrary web script or HTML via request parameters. **CVE ID : CVE-2022-27926**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Security_Center, https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P24	A-ZIM-COLL-040522/261
Vendor: Zohocorp					
Product: manageengine_adaudit_plus					
Insufficiently Protected Credentials	18-Apr-22	8.8	Zoho ManageEngine ADSelfService Plus before 6121, ADAuditPlus 7060, Exchange Reporter Plus 5701, and ADManagerPlus 7131 allow NTLM Hash disclosure during certain storage-path configuration steps. **CVE ID : CVE-2022-29457**	https://www.manageengine.com/products/self-service-password/release-notes.html, https://docs.unsafe-inline.com/0day/multiple-manageengine-applications-critical-information-disclosure-vulnerability	A-ZOH-MANA-040522/262
Product: manageengine_admanager_plus					
Insufficiently Protected Credentials	18-Apr-22	8.8	Zoho ManageEngine ADSelfService Plus before 6121, ADAuditPlus 7060, Exchange Reporter Plus 5701, and ADManagerPlus 7131 allow NTLM	https://www.manageengine.com/products/self-service-password/release-notes.html, https://docs.unsafe-	A-ZOH-MANA-040522/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hash disclosure during certain storage-path configuration steps. **CVE ID : CVE-2022-29457**	inline.com/0day/multiple-manageengine-applications-critical-information-disclosure-vulnerability	
Product: manageengine_adselfservice_plus					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Apr-22	6.8	Zoho ManageEngine ADSelfService Plus before build 6122 allows a remote authenticated administrator to execute arbitrary operating OS commands as SYSTEM via the policy custom script feature. Due to the use of a default administrator password, attackers may be able to abuse this functionality with minimal effort. Additionally, a remote and partially authenticated attacker may be able to inject arbitrary commands into the custom script due to an unsanitized password field. **CVE ID : CVE-2022-28810**	https://www.manageengine.com/products/self-service-password/kb/cve-2022-28810.html, https://github.com/rapid7/metasploit-framework/pull/16475	A-ZOH-MANA-040522/264
Insufficiently Protected Credentials	18-Apr-22	8.8	Zoho ManageEngine ADSelfService Plus before 6121, ADAuditPlus 7060, Exchange Reporter	https://www.manageengine.com/products/self-service-password/relea	A-ZOH-MANA-040522/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plus 5701, and ADManagerPlus 7131 allow NTLM Hash disclosure during certain storage-path configuration steps. **CVE ID : CVE-2022-29457**	se-notes.html, https://docs.unsafe-inline.com/0day/multiple-manageengine-applications-critical-information-disclosure-vulnerability	
Product: manageengine_exchange_reporter_plus					
Insufficiently Protected Credentials	18-Apr-22	8.8	Zoho ManageEngine ADSelfService Plus before 6121, ADAuditPlus 7060, Exchange Reporter Plus 5701, and ADManagerPlus 7131 allow NTLM Hash disclosure during certain storage-path configuration steps. **CVE ID : CVE-2022-29457**	https://www.manageengine.com/products/self-service-password/release-notes.html, https://docs.unsafe-inline.com/0day/multiple-manageengine-applications-critical-information-disclosure-vulnerability	A-ZOH-MANA-040522/266
Product: manageengine_opmanager					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-22	8.8	Zoho ManageEngine OpManager before 125588 (and before 125603) is vulnerable to authenticated SQL Injection in the Inventory Reports module. **CVE ID : CVE-2022-27908**	https://www.manageengine.com/network-monitoring/security-updates/cve-2022-27908.html	A-ZOH-MANA-040522/267
Product: manageengine_remote_access_plus					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	16-Apr-22	5.3	Zoho ManageEngine Remote Access Plus before 10.1.2137.15 allows guest users to view domain details (such as the username and GUID of an administrator). **CVE ID : CVE-2022-26653**	https://www.manageengine.com/remote-desktop-management/advisory/cve-2022-26653.html	A-ZOH-MANA-040522/268
Exposure of Resource to Wrong Sphere	16-Apr-22	5.3	Zoho ManageEngine Remote Access Plus before 10.1.2137.15 allows guest users to view license details. **CVE ID : CVE-2022-26777**	https://www.manageengine.com/remote-desktop-management/advisory/cve-2022-26777.html	A-ZOH-MANA-040522/269
Hardware					
Vendor: carrier					
Product: hills_comnav					
Inadequate Encryption Strength	20-Apr-22	5.5	Hills ComNav version 3002-19 suffers from a weak communication channel. Traffic across the local network for the configuration pages can be viewed by a malicious actor. The size of certain communications packets are predictable. This would allow an attacker to learn the state of the system if they can observe the traffic. This would be possible even if the traffic were	https://www.corporate.carrier.com/Images/CARR-PSA-Hills-ComNav-002-1121_tcm558-149392.pdf	H-CAR-HILL-040522/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encrypted, e.g., using WPA2, as the packet sizes would remain observable. The communication encryption scheme is theoretically sound, but is not strong enough for the level of protection required. **CVE ID : CVE-2022-1318**		
Improper Restriction of Excessive Authentication Attempts	20-Apr-22	5.5	There is no limit to the number of attempts to authenticate for the local configuration pages for the Hills ComNav Version 3002-19 interface, which allows local attackers to brute-force credentials. **CVE ID : CVE-2022-26519**	https://www.corporate.carrier.com/Images/CARR-PSA-Hills-ComNav-002-1121_tcm558-149392.pdf	H-CAR-HILL-040522/271
Vendor: Kyocera					
Product: d-color_mf3555					
Incorrect Authorization	20-Apr-22	8.1	An issue was discovered on Kyocera d-COLOR MF3555 2XD_S000.002.271 devices. The Web Application is affected by Broken Access Control. It does not properly validate requests for access to data and functionality under the /mngset/authset	https://kyocera.com	H-KYO-D-CO-040522/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			path. By not verifying permissions for access to resources, it allows a potential attacker to view pages that are not allowed. **CVE ID : CVE-2022-25342**		
N/A	20-Apr-22	7.5	An issue was discovered on Kyocera d-COLOR MF3555 2XD_S000.002.271 devices. The Web Application is affected by Denial of Service. An unauthenticated attacker, who can send POST requests to the /download/set.cgi page by manipulating the failhtmfile variable, is able to cause interruption of the service provided by the Web Application. **CVE ID : CVE-2022-25343**	https://kyocera.com	H-KYO-D-CO-040522/273
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-22	6.1	An XSS issue was discovered on Kyocera d-COLOR MF3555 2XD_S000.002.271 devices. The Web Application doesn't properly check parameters, sent in a /dvcset/sysset/set.cgi POST request via	https://kyocera.com	H-KYO-D-CO-040522/274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the arg01.Hostname field, before saving them on the server. In addition, the JavaScript malicious content is then reflected back to the end user and executed by the web browser. **CVE ID : CVE-2022-25344**		
Vendor: redlion					
Product: da50n					
Insufficient Verification of Data Authenticity	20-Apr-22	7.8	Authorized users may install a maliciously modified package file when updating the device via the web user interface. The user may inadvertently use a package file obtained from an unauthorized source or a file that was compromised between download and deployment. **CVE ID : CVE-2022-26516**	N/A	H-RED-DA50-040522/275
Insufficiently Protected Credentials	20-Apr-22	6.5	A malicious actor having access to the exported configuration file may obtain the stored credentials and thereby gain access to the protected resource. If the same passwords were used for other	N/A	H-RED-DA50-040522/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resources, further such assets may be compromised. **CVE ID : CVE-2022-27179**		
Operating System					
Vendor: Apple					
Product: macos					
Improper Certificate Validation	20-Apr-22	7.5	Certificate.Verify in crypto/x509 in Go 1.18.x before 1.18.1 can be caused to panic on macOS when presented with certain malformed certificates. This allows a remote TLS server to cause a TLS client to panic. **CVE ID : CVE-2022-27536**	https://groups.google.com/g/golang-announce, https://groups.google.com/g/golang-announce/c/oecdBNLOml8	O-APP-MACO-040522/277
Vendor: carrier					
Product: hills_comnav_firmware					
Inadequate Encryption Strength	20-Apr-22	5.5	Hills ComNav version 3002-19 suffers from a weak communication channel. Traffic across the local network for the configuration pages can be viewed by a malicious actor. The size of certain communications packets are predictable. This would allow an attacker to learn the state of the system if they can observe the	https://www.corporate.carrier.com/Images/CARR-PSA-Hills-ComNav-002-1121_tcm558-149392.pdf	O-CAR-HILL-040522/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic. This would be possible even if the traffic were encrypted, e.g., using WPA2, as the packet sizes would remain observable. The communication encryption scheme is theoretically sound, but is not strong enough for the level of protection required. **CVE ID : CVE-2022-1318**		
Improper Restriction of Excessive Authentication Attempts	20-Apr-22	5.5	There is no limit to the number of attempts to authenticate for the local configuration pages for the Hills ComNav Version 3002-19 interface, which allows local attackers to brute-force credentials. **CVE ID : CVE-2022-26519**	https://www.corporate.carrier.com/Images/CARR-PSA-Hills-ComNav-002-1121_tcm558-149392.pdf	O-CAR-HILL-040522/279
Vendor: Fedoraproject					
Product: fedora					
Out-of-bounds Write	18-Apr-22	7.8	global heap buffer overflow in skip_range in GitHub repository vim/vim prior to 8.2.4763. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and	https://huntr.dev/bounties/55f9c0e8-c221-48b6-a00e-bdcaebaba4a4, https://github.com/vim/vim/commit/f50808ed135ab973296bca515ae4029b321afe47	O-FED-FEDO-040522/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible remote execution **CVE ID : CVE-2022-1381**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Apr-22	5.5	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4774. **CVE ID : CVE-2022-1420**	https://github.com/vim/vim/commit/8b91e71441069b1dde9ac9ff9d9a829b1b4aecca, https://huntr.dev/bounties/a4323ef8-90ea-4e1c-90e9-c778f0ecf326	O-FED-FEDO-040522/281
Incorrect Default Permissions	18-Apr-22	5.3	A flaw was found in cri-o, where containers were incorrectly started with non-empty default permissions. A vulnerability was found in Moby (Docker Engine) where containers started incorrectly with non-empty inheritable Linux process capabilities. This flaw allows an attacker with access to programs with inheritable file capabilities to elevate those capabilities to the permitted set when execve(2) runs. **CVE ID : CVE-2022-27652**	N/A	O-FED-FEDO-040522/282
Vendor: Kyocera					
Product: d-color_mf3555_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	20-Apr-22	8.1	An issue was discovered on Kyocera d-COLOR MF3555 2XD_S000.002.271 devices. The Web Application is affected by Broken Access Control. It does not properly validate requests for access to data and functionality under the /mngset/authset path. By not verifying permissions for access to resources, it allows a potential attacker to view pages that are not allowed. **CVE ID : CVE-2022-25342**	https://kyocera.com	O-KYO-D-CO-040522/283
N/A	20-Apr-22	7.5	An issue was discovered on Kyocera d-COLOR MF3555 2XD_S000.002.271 devices. The Web Application is affected by Denial of Service. An unauthenticated attacker, who can send POST requests to the /download/set.cgi page by manipulating the failhtmfile variable, is able to cause interruption of the service provided	https://kyocera.com	O-KYO-D-CO-040522/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by the Web Application. **CVE ID : CVE-2022-25343**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-22	6.1	An XSS issue was discovered on Kyocera d-COLOR MF3555 2XD_S000.002.271 devices. The Web Application doesn't properly check parameters, sent in a /dvcset/sysset/set.cgi POST request via the arg01.Hostname field, before saving them on the server. In addition, the JavaScript malicious content is then reflected back to the end user and executed by the web browser. **CVE ID : CVE-2022-25344**	https://kyocera.com	O-KYO-D-CO-040522/285
Vendor: Oracle					
Product: solaris					
N/A	19-Apr-22	5	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris	https://www.oracle.com/security-alerts/cpuapr2022.html	O-ORA-SOLA-040522/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Solaris accessible data. CVSS 3.1 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N). **CVE ID : CVE-2022-21416**		
N/A	19-Apr-22	8.2	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). The supported version that is affected is 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpuapr2022.html	O-ORA-SOLA-040522/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			creation, deletion or modification access to critical data or all Oracle Solaris accessible data as well as unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N). **CVE ID : CVE-2022-21446**		
N/A	19-Apr-22	5.5	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Solaris accessible data. CVSS	https://www.oracle.com/security-alerts/cpuapr2022.html	O-ORA-SOLA-040522/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21461**		
N/A	19-Apr-22	5.5	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21463**	https://www.oracle.com/security-alerts/cpuapr2022.html	O-ORA-SOLA-040522/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-22	5.9	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuapr2022.html	O-ORA-SOLA-040522/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21493		
N/A	19-Apr-22	4	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 4.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21494**	https://www.oracle.com/security-alerts/cpuapr2022.html	O-ORA-SOLA-040522/291
Vendor: redlion					
Product: da50n_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	20-Apr-22	7.8	Authorized users may install a maliciously modified package file when updating the device via the web user interface. The user may inadvertently use a package file obtained from an unauthorized source or a file that was compromised between download and deployment. **CVE ID : CVE-2022-26516**	N/A	O-RED-DA50-040522/292
Insufficiently Protected Credentials	20-Apr-22	6.5	A malicious actor having access to the exported configuration file may obtain the stored credentials and thereby gain access to the protected resource. If the same passwords were used for other resources, further such assets may be compromised. **CVE ID : CVE-2022-27179**	N/A	O-RED-DA50-040522/293