History of changes in response to vulnerabilities.

Up to date as of 4/21/2026

On this page, we will compile information regarding security vulnerabilities detected in the system. Each problem listed in this table will have a CVE/CWE identifier or short description (if the vulnerability occurred in a specific part of the system), severity rating, status indicator, and the version where the issue was resolved. Vulnerabilities are listed chronologically, with the newest at the top of the list.

CVE / CWE	Detection date	Severity	Status	Versions with the fix
CVE-2026-4800 CWE-94	2026-04-08	High	Open	
CVE-2026-2950 CWE-1321	2026-04-08	Medium	Open	
CVE-2026-34601 CWE-91	2026-04-08	High	Open	
CVE-2026-4800 CWE-94	2026-04-08	High	Open	
CVE-2026-2950 CWE-1321	2026-04-08	Medium	Open	
CVE-2026-4800 CWE-94	2026-04-08	High	Open	
CVE-2026-2950 CWE-1321	2026-04-08	Medium	Open	
CVE-2026-33894 CWE-347	2026-03-31	High	Resolved	2024.1.1.347
CVE-2026-33896 CWE-295	2026-03-31	Critical	Resolved	2024.1.1.347
CVE-2026-33891 CWE-835	2026-03-31	High	Resolved	2024.1.1.347
CVE-2026-33895 CWE-347	2026-03-31	High	Resolved	2024.1.1.347
CVE-2026-33532 CWE-674	2026-03-30	Medium	Open	
CVE-2022-34716 CWE-611	2026-03-27	Medium	Open	
CVE-2018-8292 CWE-200	2026-03-27	High	Open	
CVE-2026-30227 CWE-93	2026-03-27	Medium	Open	
CWE-347	2026-03-27	Medium	Open	
CWE-189	2026-03-27	Medium	Open	
CVE-2017-9096 CWE-611	2026-03-27	High	Open	
CVE-2026-32933 CWE-674	2026-03-26	High	Open	
CVE-2026-29063 CWE-1321	2026-03-11	Critical	Resolved	2024.1.1.340;2025.2.1.321;2026.1.5.165
CVE-2025-15599 CWE-79	2026-03-11	Medium	Resolved	2024.1.1.340;2025.2.1.321;2026.1.5.165
CVE-2026-0540 CWE-79	2026-03-11	Medium	Resolved	2024.1.1.340;2025.2.1.321;2026.1.5.165
CVE-2026-2391 CWE-770	2026-02-19	Medium	Resolved	2026.1.5.164;2024.1.1.321;2025.2.1.304
CVE-2026-25128 CWE-248	2026-02-19	High	Resolved	2026.1.5.164;2024.1.1.321;2025.2.1.304

CVE-2025-69873 CWE-1333	2026-02-19	High	Resolved	2024.1.1.340;2025.2.1.321;2026.1.5.164
CVE-2026-22036 CWE-770	2026-01-27	Medium	Resolved	2026.1.4.131;2025.2.1.304;2024.1.1.321
CVE-2026-23950 CWE-176	2026-01-27	Medium	Resolved	2026.1.4.131;2025.2.1.304;2024.1.1.321
CVE-2026-23745 CWE-22	2026-01-27	Medium	Resolved	2026.1.4.131;2025.2.1.304;2024.1.1.321
CVE-2025-15284 CWE-770	2026-01-27	High	Resolved	2026.1.4.131;2025.2.1.304;2024.1.1.321
CVE-2025-54798 CWE-59	2026-01-27	Medium	Resolved	2026.1.4.131;2025.2.1.304;2024.1.1.321
CVE-2025-13465 CWE-1321	2026-01-27	Medium	Resolved	2026.1.5.164
CVE-2025-12735	2026-01-26	High	Resolved	2024.1.1.321;2025.2.1.298;2026.1.4.125
CVE-2025-13465 CWE-1321	2026-01-26	Medium	Open	
CVE-2025-13465 CWE-1321	2026-01-26	Medium	Resolved	2024.1.1.321;2025.2.1.298;2026.1.4.125
CVE-2026-22030 CWE-346	2026-01-22	Medium	Resolved	2024.1.1.321;2025.2.1.298;2026.1.4.125
CVE-2026-21884 CWE-79	2026-01-22	Medium	Resolved	2024.1.1.321;2025.2.1.298;2026.1.4.125
CVE-2025-59057 CWE-79	2026-01-22	Medium	Resolved	2024.1.1.321;2025.2.1.298;2026.1.4.125
CVE-2026-22029 CWE-79	2026-01-22	High	Resolved	2024.1.1.321;2025.2.1.298;2026.1.4.125
CVE-2025-68470 CWE-601	2026-01-22	High	Resolved	2024.1.1.321;2025.2.1.298;2026.1.4.125
CVE-2026-22611 CWE-1286	2026-01-22	Medium	Open	
A SQL Injection vulnerability was identified in the application within the parameters of business rules invoked from form rules. The lack of proper input validation and parameterization allowed an attacker to manipulate the logic of the executed database queries.	2025-12-18	High	Resolved	2025.2.1.289
An Insecure Direct Object Reference (IDOR) vulnerability was identified, allowing access to and execution of business rules based on object identifiers supplied by the user without proper authorization checks. This mechanism enabled unauthorized access to data and operations that should not be available to the affected account.	2025-12-18	Medium	Resolved	2026.1.4.125;2026.1.3.107;2025.2.1.289

A Cross-Site Scripting (XSS) vulnerability was identified that allowed the injection of malicious JavaScript code, which could then be executed in the user's browser. The vulnerability was present in the mobile application launch functionality.	2025-12-18	Medium	Resolved	2026.1.4.125;2025.2.1.293;2024.1.1.319;2026.1.3.109
CVE-2025-12816 CWE-436	2025-12-04	Critical	Resolved	2024.1.1.311;2025.2.1.274;2026.1.1.47;2026.1.2.88
CVE-2025-66400 CWE-915	2025-12-04	Medium	Resolved	2025.2.1.274
CVE-2025-64718 CWE-1321	2025-11-21	Medium	Resolved	2025.2.1.274;2024.1.1.311;2026.1.1.47
CVE-2025-64756 CWE-78	2025-11-21	High	Resolved	2025.2.1.274;2024.1.1.311;2026.1.1.47
CVE-2025-57352 CWE-1321	2025-11-21	Medium	Resolved	2024.1.1.311;2025.2.1.274;2026.1.1.47;2026.1.2.88
CVE-2025-12735 CWE-1321	2025-11-06	Critical	Resolved	2026.1.2.88;2026.1.1.45;2025.2.1.259;2024.1.1.309
CVE-2024-43483 CWE-407	2025-04-17	High	Resolved	2025.2.1.91;2024.1.1.274;2023.1.3.354
CVE-2025-22150 CWE-330	2025-04-08	High	Resolved	2024.1.1.274;2025.2.1.42;2026.1.1.45
CVE-2025-27789	2025-03-17	Medium	Resolved	2025.2.1.35;2024.1.1.248
CVE-2025-27789	2025-03-17	Medium	Resolved	2025.2.1.35;2023.1.3.354;2024.1.1.248
CVE-2025-26791 CWE-79	2025-02-28	Low	Resolved	2025.1.1.152;2024.1.1.248;2023.1.3.354;2025.2.1.35
CVE-2025-24814	2025-02-14	Medium	Resolved	2025.2.1.35
CVE-2024-52012	2025-02-14	Medium	Resolved	2025.2.1.35
CVE-2024-48510 CWE-22	2024-11-13	High	Resolved	2025.1.1.44;2023.1.3.327;2024.1.1.187
CVE-2024-43483 CWE-407	2024-10-10	High	Resolved	2024.1.1.130;2025.1.1.23
CVE-2024-43485 CWE-407	2024-10-10	High	Resolved	2024.1.1.130;2023.1.3.301;2025.1.1.23
CVE-2023-29331 CWE-400	2024-09-24	Medium	Resolved	2024.1.1.114;2023.1.3.289;2025.1.1.23
CVE-2024-4067 CWE-1333	2024-09-24	High	Resolved	2025.1.1.23
CVE-2024-45801 CWE-1321	2024-09-23	High	Resolved	2024.1.1.130;2023.1.3.289;2025.1.1.23
CVE-2024-45296 CWE-1333	2024-09-09	High	Resolved	2024.1.1.130;2023.1.3.289;2025.1.1.23
CVE-2024-35255 CWE-362	2024-08-28	Medium	Resolved	2024.1.1.114;2025.1.1.23
CVE-2024-35255 CWE-362	2024-08-28	Medium	Resolved	2024.1.1.114;2025.1.1.23
CVE-2024-29857 CWE-770	2024-08-28	Medium	Resolved	2024.1.1.114;2023.1.3.289;2025.1.1.23

CVE-2024-41818 CWE-1333	2024-07-31	Medium	Resolved	2025.1.1.23
CVE-2024-38095 CWE-20	2024-07-22	Medium	Resolved	2024.1.1.114;2023.1.3.289;2025.1.1.23
CVE-2024-30105 CWE-400	2024-07-22	High	Resolved	2024.1.1.88;2023.1.3.289;2025.1.1.23
CVE-2024-37890 CWE-400	2024-06-24	High	Resolved	2024.1.1.274;2025.2.1.42
CVE-2024-35255 CWE-362	2024-06-19	Medium	Resolved	2024.1.1.48;2023.1.3.231;2025.1.1.23
CVE-2024-35255 CWE-362	2024-06-17	Medium	Resolved	2024.1.1.48;2023.1.3.231;2025.1.1.23
CVE-2024-4067 CWE-1333	2024-05-20	High	Resolved	2024.1.1.48
CVE-2024-32028 CWE-212	2024-04-30	Medium	Resolved	2024.1.1.48;2023.1.3.289
CVE-2024-32028 CWE-212	2024-04-30	Medium	Resolved	2024.1.1.48;2023.1.3.289
CVE-2024-29992 CWE-522	2024-04-30	Medium	Resolved	2023.1.3.231;2024.1.1.48
CWE-1336	2024-04-19	Medium	Resolved	2023.1.3.169;2024.1.1.48
CVE-2024-28863 CWE-400	2024-03-25	Medium	Resolved	2024.1.1.48
CVE-2023-29331 CWE-400	2024-02-19	High	Resolved	2023.1.3.202;2024.1.1.48
CVE-2023-26115 CWE-1333	2024-02-13	Low	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2023-28154 CWE-265	2024-02-13	High	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2023-26136 CWE-1321	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-25858 CWE-1333	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CWE-79	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-25883 CWE-1333	2024-02-13	High	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2023-44270 CWE-20	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-3517 CWE-1333	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-37603 CWE-1333	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-37601 CWE-1321	2024-02-13	High	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-37599 CWE-1333	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-46175 CWE-1321	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48

CWE-772	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2023-26159 CWE-20	2024-02-13	High	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2023-45133 CWE-184	2024-02-13	Critical	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-39353 CWE-20	2024-02-13	Critical	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-37616 CWE-1321	2024-02-13	High	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-23539 CWE-327	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-23541 CWE-1259	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CVE-2022-23540 CWE-287	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404;2024.1.1.48
CWE-772	2024-01-29	Medium	Resolved	2024.1.1.48
CVE-2024-0056 CWE-420	2024-01-23	High	Resolved	2023.1.3.118
CVE-2024-21319 CWE-400	2024-01-10	Medium	Resolved	2023.1.3.76;2024.1.1.48
CVE-2023-36414 CWE-94	2023-10-10	High	Resolved	2023.1.2.123;2022.1.4.346;2023.1.3.29
CVE-2023-4863 CWE-122	2023-09-11	Critical	Resolved	2023.1.2.99;2022.1.4.326;2023.1.3.29
Fixed a bug where the security system, designed to protect against Cross-Site Request Forgery (CSRF) attacks, failed to start despite the correct configuration.	2023-07-26	High	Resolved	2022.1.4.288;2023.1.2.44;2023.1.3.29
CVE-2023-29337 CWE-94	2023-06-14	High	Resolved	2023.1.2.44
CWE-400	2023-06-14	High	Resolved	2023.1.2.44
CVE-2023-21893 CWE-284	2023-04-16	High	Resolved	2023.1.1.89;2023.1.2.44
CVE-2022-46175	2022-12-25	Medium	Resolved	2022.1.4.127;2023.1.1.41
Fixed an issue in WEBCON BPS Portal that allowed a non-administrator user to assign different types of privileges to other users.	2022-12-21	Critical	Resolved	2021.1.4.354;2022.1.4.155;2023.1.1.41
CVE-2022-23494 CWE-79	2022-12-09	Medium	Resolved	2023.1.1.41
18 security vendors and no sandboxes flagged the BouncyCastle.Crypto.dll file as malicious	2022-11-09	Medium	Resolved	2022.1.4.111;2021.1.4.344;2023.1.1.41
CVE-2022-41064 CWE-200	2022-11-09	Medium	Resolved	2023.1.1.41
CVE-2022-41032	2022-10-11	High	Resolved	2023.1.1.41
CVE-2022-051	2022-09-15	Medium	Resolved	2022.1.2.31

CWE-319	2022-08-31	Medium	Resolved	2022.1.4.47
Added support for CORS (Cross-Origin Resource Sharing).	2022-08-10	Medium	Resolved	2022.1.4.47
CVE-2022-34716	2022-08-09	Medium	Resolved	2023.1.1.41
CVE-2022-31129 CWE-1333	2022-07-06	High	Resolved	2021.1.4.292;2022.1.3.47
CVE-2022-30184 CWE-200	2022-06-14	Medium	Resolved	2022.1.3.47
CVE-2021-24112 CWE-94	2022-05-24	High	Resolved	2023.1.2.44
Ddded configurations for protection against CSRF attacks (Cross Site Request Forgery, XSRF), and the ability to configure a list of endpoints that will not be checked for CSRF.	2022-05-19	Medium	Resolved	2022.1.3.47
Added protection against HTML script injection on Portal.	2022-04-28	Medium	Resolved	2022.1.3.47
CWE-755	2022-04-24	High	Resolved	2022.1.3.47
CWE-755	2022-04-24	High	Resolved	2023.1.1.41
CWE-755	2022-04-24	High	Resolved	2022.1.3.47
CVE-2022-24785	2022-04-05	High	Resolved	2021.1.4.223;2022.1.3.47
Added ability to configure the lifetime of access tokens and authentication cookies	2022-03-18	Medium	Resolved	2022.1.2.31;2022.1.3.47
CVE-2022-0686	2022-02-21	Medium	Resolved	2021.1.4.165;2022.1.2.31
CVE-2022-0691	2022-02-21	High	Resolved	2021.1.4.165;2022.1.2.31
CVE-2022-0686	2022-02-21	Medium	Resolved	2021.1.4.195
CVE-2022-0691	2022-02-21	High	Resolved	2021.1.4.195
CVE-2022-0512	2022-02-15	Medium	Resolved	2021.1.4.165;2022.1.2.31
CVE-2022-0512	2022-02-15	Medium	Resolved	2021.1.4.195
Support for connections without HTTPS / SSL has been disabled in the iOS and Android mobile applications.	2022-01-19	Medium	Resolved	2022.1.2.31
CVE-2021-44228	2021-12-10	Critical	Resolved	2021.1.4.154;2022.1.1.41
CVE-2021-46708	2021-12-09	Medium	Resolved	2023.1.2.44

CVE-2018-25031 CWE-918	2021-12-09	Medium	Resolved	2023.1.2.44
The useunsafeheaderparsing flag in the REST action has been removed	2021-12-02	Medium	Resolved	2022.1.1.41
Changed the display conditions for certain system errors. Such security measures will ensure that a user does not see an error containing sensitive details (e.g. SQL queries).	2021-06-29	Medium	Resolved	2021.1.4.36
For all REST API methods, custom headers will be added	2021-06-15	Medium	Resolved	2022.1.1.41
Security fixes have been introduced to protect websites from Cross-Site Scripting (XSS) attacks by appropriate coding of potentially dangerous places based on Microsoft's recommendations.	2021-05-19	Medium	Resolved	2022.1.2.31
Swagger component version has been upgraded. This change introduces the latest security fixes for this component.	2021-05-17	Medium	Resolved	2021.1.3.163
Updated a version of the SOLR search engine to 8.8.2 and a version of Java libraries to 16.0.1. This change introduces the latest performance and security improvements of those components.	2021-04-30	Medium	Resolved	2021.1.3.163
CVE-2021-26701 CWE-94	2021-04-21	Critical	Resolved	2022.1.3.47
CVE-2021-26701 CWE-94	2021-04-21	Critical	Resolved	2022.1.3.47
CVE-2019-0820 CWE-400	2019-05-14	High	Resolved	2022.1.3.47
CVE-2019-0820 CWE-400	2019-05-14	High	Resolved	2022.1.3.47
CVE-2019-0820 CWE-400	2019-05-14	High	Resolved	2022.1.3.47
CVE-2018-8292 CWE-200	2018-10-10	High	Resolved	2022.1.3.47
CVE-2018-8292 CWE-200	2018-10-10	High	Resolved	2022.1.3.47
CVE-2017-0256 CWE-20	2017-05-12	Medium	Resolved	2022.1.3.47
CVE-2017-0249 CWE-269	2017-05-12	High	Resolved	2022.1.3.47
CVE-2017-0248 CWE-287	2017-05-12	High	Resolved	2022.1.3.47

CVE-2017-0247 CWE-254	2017-05-09	High	Resolved	2022.1.3.47