History of changes in response to vulnerabilities.

Up to date as of 14.06.2024

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-2024-4067 CWE-1333	2024-05-20	High	Open	
CVE-2024-32028 CWE-212	2024-04-30	Medium	Open	
CVE-2024-32028 CWE-212	2024-04-30	Medium	Open	
CVE-2024-29992 CWE-522	2024-04-30	Medium	Open	
CWE-1336	2024-04-19	Medium	Resolved	2023.1.3.169
CVE-2024-28863 CWE-400	2024-03-25	Medium	Open	
CVE-2023-29331 CWE-400	2024-02-19	High	Resolved	2023.1.3.202
CVE-2023-26115 CWE-1333	2024-02-13	Low	Resolved	2023.1.3.118;2022.1.4.404
CVE-2023-28154 CWE-265	2024-02-13	High	Resolved	2023.1.3.118;2022.1.4.404
CVE-2023-26136 CWE-1321	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CVE-2022-25858 CWE-1333	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CWE-79	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CVE-2022-25883 CWE-1333	2024-02-13	High	Resolved	2023.1.3.118;2022.1.4.404
CVE-2023-44270 CWE-20	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CVE-2022-3517 CWE-1333	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CVE-2022-37603 CWE-1333	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CVE-2022-37601 CWE-1321	2024-02-13	High	Resolved	2023.1.3.118;2022.1.4.404
CVE-2022-37599 CWE-1333	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CVE-2022-46175 CWE-1321	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CWE-772	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CVE-2023-26159 CWE-20	2024-02-13	High	Resolved	2023.1.3.118;2022.1.4.404
CVE-2023-45133 CWE-184	2024-02-13	Critical	Resolved	2023.1.3.118;2022.1.4.404
CVE-2022-39353 CWE-20	2024-02-13	Critical	Resolved	2023.1.3.118;2022.1.4.404
CVE-2022-37616 CWE-1321	2024-02-13	High	Resolved	2023.1.3.118;2022.1.4.404

CVE-2022-23539 CWE-327	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CVE-2022-23541 CWE-1259	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CVE-2022-23540 CWE-287	2024-02-13	Medium	Resolved	2023.1.3.118;2022.1.4.404
CWE-772	2024-01-29	Medium	Open	
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
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	2023.1.1.41;2022.1.4.127
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	2023.1.1.41;2021.1.4.354;2022.1.4.155
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	2023.1.1.41;2022.1.4.111;2021.1.4.344
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	2023.1.1.41;2022.1.2.31
CWE-319	2022-08-31	Medium	Resolved	2023.1.1.41;2022.1.4.47
Added support for CORS (Cross-Origin Resource Sharing).	2022-08-10	Medium	Resolved	2023.1.1.41;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	2023.1.1.41;2021.1.4.292;2022.1.3.47
CVE-2022-30184 CWE-200	2022-06-14	Medium	Resolved	2023.1.1.41;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	2023.1.1.41;2022.1.3.47
Added protection against HTML script injection on Portal.	2022-04-28	Medium	Resolved	2023.1.1.41;2022.1.3.47
CWE-755	2022-04-24	High	Resolved	2023.1.1.41;2022.1.3.47
CWE-755	2022-04-24	High	Resolved	2023.1.1.41
CWE-755	2022-04-24	High	Resolved	2023.1.1.41;2022.1.3.47
CVE-2022-24785	2022-04-05	High	Resolved	2023.1.1.41;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	2023.1.1.41;2022.1.2.31;2022.1.3.47
CVE-2022-0686	2022-02-21	Medium	Resolved	2023.1.1.41;2021.1.4.165;2022.1.2.31
CVE-2022-0691	2022-02-21	High	Resolved	2023.1.1.41;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	2023.1.1.41;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	2023.1.1.41;2022.1.2.31
CVE-2021-44228	2021-12-10	Critical	Resolved	2022.1.1.41;2021.1.4.154
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	2022.1.1.41;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	2023.1.1.41;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	2022.1.1.41;2021.1.3.163
CVE-2021-26701 CWE-94	2021-04-21	Critical	Resolved	2023.1.1.41;2022.1.3.47
CVE-2021-26701 CWE-94	2021-04-21	Critical	Resolved	2023.1.1.41;2022.1.3.47
CVE-2019-0820 CWE-400	2019-05-14	High	Resolved	2023.1.1.41;2022.1.3.47
CVE-2019-0820 CWE-400	2019-05-14	High	Resolved	2023.1.1.41;2022.1.3.47
CVE-2019-0820 CWE-400	2019-05-14	High	Resolved	2023.1.1.41;2022.1.3.47
CVE-2018-8292 CWE-200	2018-10-10	High	Resolved	2023.1.1.41;2022.1.3.47
CVE-2018-8292 CWE-200	2018-10-10	High	Resolved	2023.1.1.41;2022.1.3.47
CVE-2017-0256 CWE-20	2017-05-12	Medium	Resolved	2023.1.1.41;2022.1.3.47
CVE-2017-0249 CWE-269	2017-05-12	High	Resolved	2023.1.1.41;2022.1.3.47
CVE-2017-0248 CWE-287	2017-05-12	High	Resolved	2023.1.1.41;2022.1.3.47
CVE-2017-0247 CWE-254	2017-05-09	High	Resolved	2023.1.1.41;2022.1.3.47