Security Advisories

Publishing Policy

When a critical severity security vulnerability is discovered and resolved, we will inform customers through the following mechanisms:

- We will post a security advisory on https://confluence.xpand-it.com/display/XPORTER/Security+Advisories at the same time as releasing a fix for the vulnerability.
- We will send an email copy of all critical security advisories to the technical contacts we have in our database.

If you want to track non-critical severity security vulnerabilities, you need to monitor the issue trackers for the relevant products on https://jira.xpand-it.com/, for example, https://jira.xpand-it.com/browse/XPORTER for Xporter for Jira Server and Data Center. Security issues are marked with security labels: security_vulnerability_critical, security_vulnerability_high, security_vulnerability_medium, security_vulnerability_low).

All security issues will be listed in the release notes of the release where they have been fixed, similar to other bugs.

Advisories

- Security Advisory 2020-04-29 - Blind SQL Injection on the Audit Log and RCE on Post Functions and Scheduled Reports
- Security Advisory - July, 2021
- Security Advisory - March, 2022
- Security Advisory - May, 2022

List of Know Security Vulnerabilities for Xporter

Key	Summary	T	Created	Status	Affected Version/s	Fix Version/s	Labels
XPORTER-3776	Remote Code Execution - Templates Export		May 21, 2021	CLOSED	Release 2.9.5	6.7.3	ignore_coverage security_vulnerability_critical
XPORTER-3735	Remote Code Execution - Export and Import Settings		Apr 20, 2021	CLOSED	Release 5.2.0	6.7.2	security_vulnerability_critical
XPORTER-3733	Local File Disclosure - Template file		Apr 19, 2021	CLOSED	Release 2.9.5	6.7.2	security_vulnerability_critical
XPORTER-3732	SQL Injection - Administration Process Manager		Apr 19, 2021	CLOSED	Release 6.2.0	6.7.2	security_vulnerability_critical
XPORTER-3731	SQL Injection - My Exports		Apr 19, 2021	CLOSED	Release 6.2.0	6.7.2	security_vulnerability_critical
XPORTER-3730	SQL Injection - Administration Audit Log		Apr 19, 2021	CLOSED	Release 5.7.0	6.7.2	security_vulnerability_critical
XPORTER-3157	RCE vulnerability at Multi-action Workflow Post Function		Feb 24, 2020	CLOSED	Release 5.5.0	6.3.4	security_vulnerability_critical
XPORTER-2959	RCE vulnerability at Scheduled Report		Dec 04, 2019	CLOSED	5.0.0	6.3.4	security_vulnerability_critical
XPORTER-2958	Blind SQL injection at Audit Log		Dec 04, 2019	CLOSED	Release 5.7.0	Release 6.3.0	security_vulnerability_critical
XPORTER-3644	IDOR Leads to unauthorized user perform operations on templates, audit log and settings		Feb 12, 2021	CLOSED	6.6.7	6.6.8	security_vulnerability_high vulnerability
XPORTER-3496	REST API endpoint Leaked sensitive information		Oct 13, 2020	CLOSED	Release 4.3.0	6.6.0	security_vulnerability_high
XPORTER-3207	REST API CSRF		Mar 12, 2020	CLOSED	6.3.4	6.7.1	security_vulnerability_high vulnerability
XPORTER-3179	Site-wide CSRF on Xporter actions and pages		Feb 26, 2020	CLOSED	5.0.0	6.3.4	security_vulnerability_high
XPORTER-3159	Xporter returns sensitive information on File Servers Rest Service.		Feb 24, 2020	CLOSED	Release 4.3.0	6.3.4	security_vulnerability_high

XPORTER-2956	Unauthenticated user can access, create, update, delete template		Dec 04, 2019	CLOSED	Release 6.2.4	Release 6.3.0	security_vulnerability_high
XPORTER-3609	Stored XSS at Xporter on My export list by user profile name		Dec 22, 2020	CLOSED	Release 6.2.0	6.6.6	security_vulnerability_low
XPORTER-3526	REST API endpoint on Leaked Confluence data		Oct 22, 2020	CLOSED		6.6.3, Continuous Delivery	security_vulnerability_low
XPORTER-3525	REST API endpoint Leaked Confluence Spaces		Oct 22, 2020	CLOSED		6.6.3, Continuous Delivery	security_vulnerability_low
XPORTER-3524	Users with "user" privilege can see all the permission schemes created in the Jira instance		Oct 22, 2020	CLOSED		6.6.3, Continuous Delivery	security_vulnerability_low
XPORTER-3523	Users with "user" privilege can see all the File Server created in the Jira instance		Oct 22, 2020	CLOSED		6.6.3, Continuous Delivery	security_vulnerability_low

Showing 20 out of 29 issues