Security Advisories

#	Title	Date	Severity	Description
1	MidPoint user interface clickjacking	21 Mar 2019	Medium	MidPoint user interface vulnerable to clickjacking due to missing X-Frame-Options header.
2	Abuse of expressions in midPoint reports	8 Apr 2019	Medium	MidPoint expressions embedded in midPoint reports can be used to gain unauthorized access to the system.
3	XXE Vulnerabilities	17 Apr 2019	Medium	The way how MidPoint handles XML documents is vulnerable to attacks based on XML External Entities (XXE)
4	AD and LDAP connectors do not check certificate validity	17 Apr 2019	High	LDAP and Active Directory connectors are not properly checking TLS/SSL certificate validity.
5	Workitem identifier weakness	18 Apr 2019	Medium	Any approver can display any workitem by guessing its short identifier.
6	Plain text password in temporary files	13 May 2019	Low	Plaintext password is sometimes left stored in temporary files on a file system.
7	Plain text password in task objects in repository	23 May 2019	Low	Plaintext passwords are sometimes stored in task objects in the repository (database).
8	XSS Vulnerability In displayName	14 Jun 2019	Low	Cross-site scripting (XSS) vulnerability exists in some parts of midPoint user interface, namely in organization displayName.
9	SOAP Web Service Vulnerable To Brute Force Attack	9 Jul 2019	Medium	SOAP-based web service interface of midPoint does not limit authentication attempts.
10	Authorizations not applied properly to preview changes	30 Jul 2019	Medium	Authorizations not applied properly to the results of "preview changes" functionality.
11	Stored XSS vulnerability via 'name' property	30 Aug 2019	Medium	Stored cross-site scripting (XSS) vulnerability exists in midPoint user interface that can be exploited by manipulation of object 'name' property.
12	User changes and user session updates	9 Sep 2019	Low	Sessions of users logged-in to midPoint user interface are unaffected by the change of user profiles - until users log in again.
13	HTTP error codes used for SecQ REST authentication reveal user existence	11 Oct 2019	Low	HTTP error codes used for REST authentication based on security questions (a.k.a. SecQ) reveal user existence.