SecurityAdvisories

This is the advisory page for Service Provider V3 releases. For older V2 SP advisories, refer to the V2 SecurityAdvisories page.

This page provides access to the complete history of Security Advisories released for the Shibboleth V3 Service Provider and an "at a glance" table showing you which releases are vulnerable to what kinds of issues. If you're running a particular version, you can use this table to identify the issues that could affect your system and determine how urgent an upgrade is. In addition to the announce mailing list, you can "watch" this page for changes to keep abreast.

You can determine the exact version you're running based on the shibd.log during startup.

If you would like to report an issue you believe is security related, please drop an e-mail to security@shibboleth.net

As always, sites are advised to use the latest stable release of any Shibboleth product. Refer to the ProductVersioning page for information about our support and versioning policies. The Home page identifies the specific versions recommended at a given point in time

This page **only** covers advisories affecting the V3 Service Provider software. Other advisories are not listed here, but you can find the complete set of advisories in this directory.

Obviously not all vulnerabilities are created equal, and the classifications in the matrices are general in nature, and are meant to point you to the relevant advisories to look into.

A particular version will typically be implicated by any advisories noted for it and for any newer versions above it in the tables.

Advisories noted for "All" versions should be reviewed by all deployers for relevancy to their deployment. Typically this indicates that an advisory is at least partly discussing issues that go beyond the scope of what the Shibboleth software can actually remediate and may affect the deployment as a whole. It does not in general refer to unfixed vulnerabilities in the Shibboleth software itself.

Service Provider Vulnerability Matrix

The oldest SP 3 version unaffected by fixable vulnerabilities is **3.2.2**.

Version	EOL	User Data Exposure	Resource Exposure	Session Hijacking	Denial of Service	Remote Exploit	Advisories
All		X	X		X	X	2018-08-03, 2018-01-23, 2014-04-09, 2011-10-24
3.2.2							
3.2.1	Apr 2021				X		2021-04-26
3.2.0	Mar 2020				X		2020-03-17
3.1.0	Dec 2020				X		2020-08-31
3.0.4	Apr 2020				X		
3.0.3	Mar 2019				X		2019-03-11
3.0.2	Dec 2018				X		2018-12-19a
3.0.1	Aug 2018	X	X		X	X	
3.0.0	Jul 2018				X		

Advisory List

Date	Title	Affects	Severity	CVE
2021-04-26	Session recovery feature contains a null pointer deference	SP < 3.2.2	moderate	
2020-03-17	Template generation allows external parameters to override placeholders	SP < 3.2.1	moderate	
2020-08-31	IIS module fails to trap exceptions raised by network socket failures	SP for Windows IIS7+ module < 3.1.0.2	moderate	
2019-03-11	XML parser class fails to trap exceptions on malformed XML declaration	SP w/ libxmltooling < 3.0.4	moderate	CVE-2019-9628
2018-12-19	Shibboleth SP software crashes on malformed date/time content	SP < 3.0.3	moderate	
2018-08-03	Shibboleth SP software crashes on malformed KeyInfo content	SP w/ libxml-security-c < 2.0.2	high	

2018-01-23	Implications of ROBOT TLS vulnerability	All	high	
2014-04-09	OpenSSL "Heartbleed" vulnerability	SP or IDP w/ OpenSSL 1.0.1 - 1.0.1f	very high	CVE-2014-0160
2011-10-24	Use of XML Encryption Vulnerable to Chosen Ciphertext Attacks	SP and IdP, all versions	moderate	