

Advisory
6 minutes read

TYPO3 Cross-Site Scripting Vulnerability

Purplemet Lab
October 21, 2019

Vulnerability

Purplemet Lab team discovered a cross-site scripting (XSS) vulnerability in TYPO3 6.2.0 to 6.2.38 ELTS and TYPO3 7.0.0 to 7.1.0 (CVE-2020-8091). These versions embed a third party component named SVG Web which provides svg.svg, a Flash file vulnerable to a cross-site scripting.

Solution

Update to TYPO3 6.2.39 ELTS or latest version for 6.2.x and TYPO3 7.x latest version. This component has been removed in 7.2 - see the [commit](#).

Proof of concept

The vulnerability can be triggered using the following URL:















```
http://ip/typo3/contrib/websvg/svg.svg?uniqueId=%22}})catch(e)
!s,x=1}//
```

Reference

See TYPO3 Security Advisory [TYPO3-PSA-2019-003](#).

Purplemet technology detection

Purplemet detects TYPO3 and flags SVG Web as Unsafe component.

name	component	version	risk	last
	Apache	Web Server	0	
	ExtJS	JavaScript Library	3.4.0	0
	jQuery	JavaScript Library	0	
	Lightbox	JavaScript Library	2.71	0
	Linux	Operating System	3.2-9-6-arch64 #1 SMP Debian 3.2...	0
	Moodle	JavaScript Library	1.6	0
	OpenSSL	Web Server Extension	1.0.1g 3 May 2015	0
	PHP	Programming Language	5.4.45-0+deb7u8	0
	Prototype	JavaScript Library	1.7.0	0
	SVG Web	JavaScript Library	0	Unsafe
	TYPO3	Miscellaneous	0	
	jQuery	JavaScript Library	0	
	TYPO3 CMS	CMS	6.2	0
	TYPO3 CMS Administration Console	CMS	0	Unsafe

Up Next

Palo Alto Firewall
Multiple Cross-Site Scripting Vulnerabilities

Purplemet Lab
November 28, 2019