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-2020-869]). These versions embed a third party component named SVG Web which provides svg.swf, a Flash file vulnerable to a cross-site scripting.

Solution

Update to TYPO3 6.2.39 ELTS or latest version for 6.2x and TYPO3 7x latest version. This component has been removed in 72 - see the commit.

Proof of concept

The vulnerability can be triggered using the following URL:

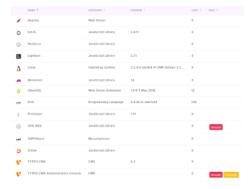
http://ip/typo3/contrib/websvg/svg.swf?uniqueId=%22])}catch(e) iis.x=1}//

Reference

See TYPO3 Security Advisory TYPO3-PSA-2019-003.

Purplemet technology detection

Purplemet detects TYPO3 and flags SVG Web as Unsafe component.



Up Next

Palo Alto Firewall Multiple Cross-Site Scripting Vulnerabilities

Purplemet Lab November 28, 2019

 Product
 Company
 Contact

 Features
 Blog
 Get in touch

 Solution
 Legal
 Twitter

 Plans
 Privacy
 Linkedin

 Putners
 Terms of use