



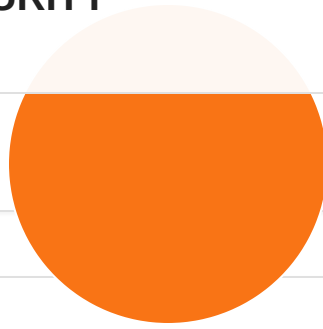
Main > Vulnerability Database > SB2012070701

SB2012070701 - Arbitrary file upload in scribu Front-end Editor for WordPress

Published: July 7, 2012

Security Bulletin ID	SB2012070701
Severity	High
Patch available	<input checked="" type="checkbox"/> YES
Number of vulnerabilities	1
Exploitation vector	Remote access
Highest impact	Code execution

Breakdown by Severity



High 100%

Description

■ Low ■ Medium ■ High ■ Critical

This security bulletin contains information about 1 security vulnerability.

1) Arbitrary file upload (CVE-ID: N/A)

The vulnerability allows a remote attacker to compromise vulnerable system. The vulnerability exists due to insufficient validation of file extension when uploading files. A remote attacker can upload and execute arbitrary file on the system.

Remediation

Install update from vendor's website.

References

- <https://web.archive.org/web/20120712205339/>
- <http://www.opensyscom.fr/Actualites/wordpress-plugins-front-end-editor-arbitrary-file-upload-vulnerability.html>

Vulnerable Software



[Terms of Use](#) | [Privacy Policy](#) | [Contacts](#)

© 2026 Cybersecurity Help s.r.o.