GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

31 August 2026

Advisory 209: Form Maker by 10Web Unauthenticated Cross-Site Scripting (XSS) Vulnerability (CVE-2026-66616).

Release Date: 21st August 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to website administrators and developers who use the Form Maker by 10Web WordPress plugin. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-66616 is a high-severity, unauthenticated cross-site scripting (XSS) vulnerability in "Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder", a widely used WordPress plugin. Insufficient input sanitisation and output escaping allow a malicious script to be injected into a form field and later executed in a visitor's browser when the affected page is viewed.

Exploitation does not require an attacker account, but does require a victim to interact with a crafted link or page - for example a site visitor, or an administrator viewing submitted form data. The vulnerability carries a CVSS 3.1 score of 7.1 (High) and is classified as CWE-79 (Improper Neutralization of Input During Web Page Generation, Cross-Site Scripting). Its "Scope: Changed" rating means the injected script can affect data or components beyond the vulnerable form itself.

What are the systems affected?

The following plugin and version(s) are affected:

- Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder (WordPress plugin), versions up to and including 1.15.46 – (Affected)

No patched version is currently available. 1.15.46 remains the latest release published on WordPress.org at the time of this advisory, and the plugin has more than 30,000 active installations.

What does this mean?

Typical attack flow:

1. **Attacker crafts a malicious payload**
    - The attacker prepares a script payload and delivers it through a Form Maker field or a crafted link to the affected page — no authentication or plugin access is needed.
2. **Victim interacts with the crafted content**
    - A site visitor opens the affected page, or an administrator views the submitted form data, causing the unsensitized script to execute in their browser under the site's own origin.

Attack vectors:

- Malicious links shared via email, social media or messaging apps that point to the vulnerable form/page
- Malicious content submitted directly through the form itself, if reflected or later viewed unsensitised

Successful exploitation allows attackers to:

- Inject redirects, adverts or other unwanted HTML content that visitors see when they load the affected page
- Hijack an administrator's active session if they trigger the payload while logged in, given the vulnerability's "Scope: Changed" rating — a path to full site compromise

Mitigation process

CERTVU recommends the following:

1. Monitor for and Apply an Official Patch

- No fixed version has been released as of this advisory. Watch the Form Maker by 10Web changelog on WordPress.org and update to a patched release as soon as one is published.
- If your site is a Patchstack customer, confirm the interim virtual-patching rule for this CVE is active.

2. Deploy a compensating WAF/virtual-patch rule for this CVE if immediate updating is not possible, as an interim measure only.
3. Advise Administrators on Session Hygiene

- Instruct administrators not to click unsolicited or untrusted links while logged in to the WordPress admin panel, given the risk of session hijacking.

4. Monitor for Signs of Exploitation

- Watch for unexpected redirects, adverts or injected content on pages using Form Maker, and review form submissions for suspicious script content.

5. Consider temporarily deactivating the plugin if it is not business-critical, until a patched version is released.

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-66616
2. https://patchstack.com/database/wordpress/plugin/form-maker/vulnerability/wordpress-form-maker-by-10web-plugin-1-15-46-cross-site-scripting-xss-vulnerability