Advisory Summary

Dolibarr ERP & CRM v14.0.2 suffers from a stored XSS vulnerability in the ticket creation flow that allows a low level user (with full access to the Tickets module) to achieve full permissions. For this attack vector to work, an administrator user needs to copy the text in the "message" box.

Impact

Authenticated attackers could perform actions in the context of high privilege users. This vulnerability could lead to site-wide account takeovers, privilege escalation and Anti-CSRF tokens pillage.

Affected Vendor

Vendor	Product
Dolibarr	Dolibarr ERP CRM 14.0.2 and earlier versions

Vulnerability Summary

The built-in WAF (Web application Firewall) uses a deny list to block the some HTML tags and most JavaScript events except for `onbeforecopy` and `onbeforecut` . In order to exploit this vulnerability, an authenticated attacker needs to craft a payload that does not include any of the forbidden HTML tags and JavaScript events.

```
// For XSS Injection done by closing textarea to execute content into a textarea field

 $inj += preg_match('/<\/textarea/i', $val);



 $inj += preg_match('/<audio/i', $val);

 $inj += preg_match('/<embed/i', $val);

 $inj += preg_match('/<iframe/i', $val);
 $inj += preg_match('/<object/i', $val);

 $inj += preg_match('/<script/i', $val);

 $inj += preg_match('/Set\.constructor/i', $val); // ECMA script 6

 if (!defined('NOSTYLECHECK')) {

 $inj += preg_match('/<style/i', $val);

 }

 $inj += preg_match('/base\s+href/si', $val);

 $inj += preg_match('/=data:/si', $val);

 $inj += preg_match('/on(mouse|drag|key|load|touch|pointer|select|transition)
([a-z]*)\s*=/i', $val); // onmousexxx can be set on img or any html tag like
<img title='...' onmouseover=alert(1)>

 $inj +=
preg_match('/on(abort|afterprint|animation|auxclick|beforeprint|beforeunload|blur
 $val);

 $inj +=
preg_match('/on(dblclick|drop|durationchange|emptied|ended|error|focus|focusin|foc
 $val);

 $inj +=
preg_match('/on(lostpointercapture|offline|online|pagehide|pageshow)\s*=/i',
$val);

 $inj +=
preg_match('/on(paste|pause|play|playing|progress|ratechange|reset|resize|scroll|
 $val);

 $inj +=
preg_match('/on(timeupdate|toggle|unload|volumechange|waiting|wheel)\s*=/i',
$val);
```

```
 $tmpval = preg_replace('/<[^<]+>/', '', $val);

 // List of dom events is on https://www.w3schools.com/jsref/dom_obj_event.asp
and https://developer.mozilla.org/en-US/docs/Web/API/GlobalEventHandlers

 $inj += preg_match('/on(mouse|drag|key|load|touch|pointer|select|transition)
([a-z]*)\s*=/i', $val); // onmousexxx can be set on img or any html tag like
<img title='...' onmouseover=alert(1)>

 $inj +=
preg_match('/on(abort|afterprint|animation|auxclick|beforeprint|beforeunload|blur
 $tmpval);


 $inj +=
preg_match('/on(dblclick|drop|durationchange|emptied|ended|error|focus|focusin|foc
 $tmpval);

 $inj +=
preg_match('/on(lostpointercapture|offline|online|pagehide|pageshow)\s*=/i',
$tmpval);

 $inj +=
preg_match('/on(paste|pause|play|playing|progress|ratechange|reset|resize|scroll|s
 $tmpval);

 $inj +=
preg_match('/on(timeupdate|toggle|unload|volumechange|waiting|wheel)\s*=/i',
$tmpval);
```

Deny list implemented in main.inc.php line 87.

Proof of Concept

We have released a proof of concept in the following sources:

- https://www.exploit-db.com/exploits/50432
- https://packetstormsecurity.com/files/164544/Dolibarr-ERP-CRM-14.0.2-Cross-Site-Scripting-Privilege-Escalation.html

Solution

Update to newest version.

Timeline

- 10/8/2021 - Contact with vendor.
- 10/8/2021 - Vulnerability acknowleged and fix released.