

@ArmySick

twitter

github

CVE-2021-33231 — Stored XSS in EasyVista Service Manager

May 7, 2021

cve

xss

easyvista

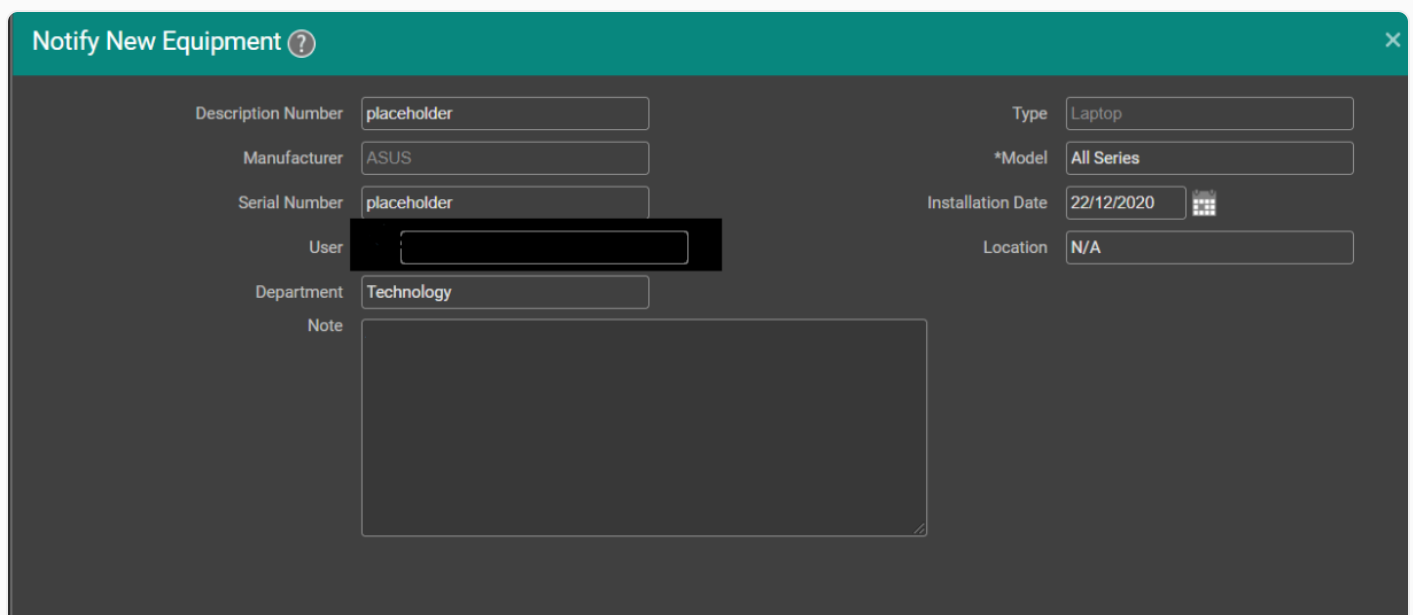
Overview

A stored cross-site scripting (XSS) is available when registering a new equipment on EasyVista Service Manager 2018.1.181.1, on the Note field, allowing arbitrary JavaScript code to be executed on any user that visits the details page of the registered equipment.

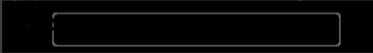
A filter is in place that attempts to prevent this, but it is incomplete, which makes it bypassable.

Details

After logging into the platform, a user is able to, among other functions, consult its own equipment. There is also a function available that allows registration of new equipment:



Notify New Equipment ?

Description Number	placeholder	Type	Laptop
Manufacturer	ASUS	*Model	All Series
Serial Number	placeholder	Installation Date	22/12/2020 
User		Location	N/A
Department	Technology		
Note			

In the “Note” field there are protections in-place that correctly disallow (through filtering) the usage of JavaScript tags such as `<script>`. However, it is possible to bypass it and inject valid JavaScript code by using different syntaxes that do not use the `<script>` tag.

The payload tested, shown below, was `<img src=x onerror="alert('xss')"/>`:

Service Manager Search or type a command

My Favorites

General

My Data

My Contracts

My Details

My Equipment

My Department

Full Text Search

Service Operation

My Equipment

Notify New Equipment

Description Number placeholder

Manufacturer ASUS

Serial Number placeholder

User [REDACTED]

Department Technology

Note `<img src=x onerror='alert('xss')'/>`

Type Laptop

*Model All Series

Installation Date 22/12/2020

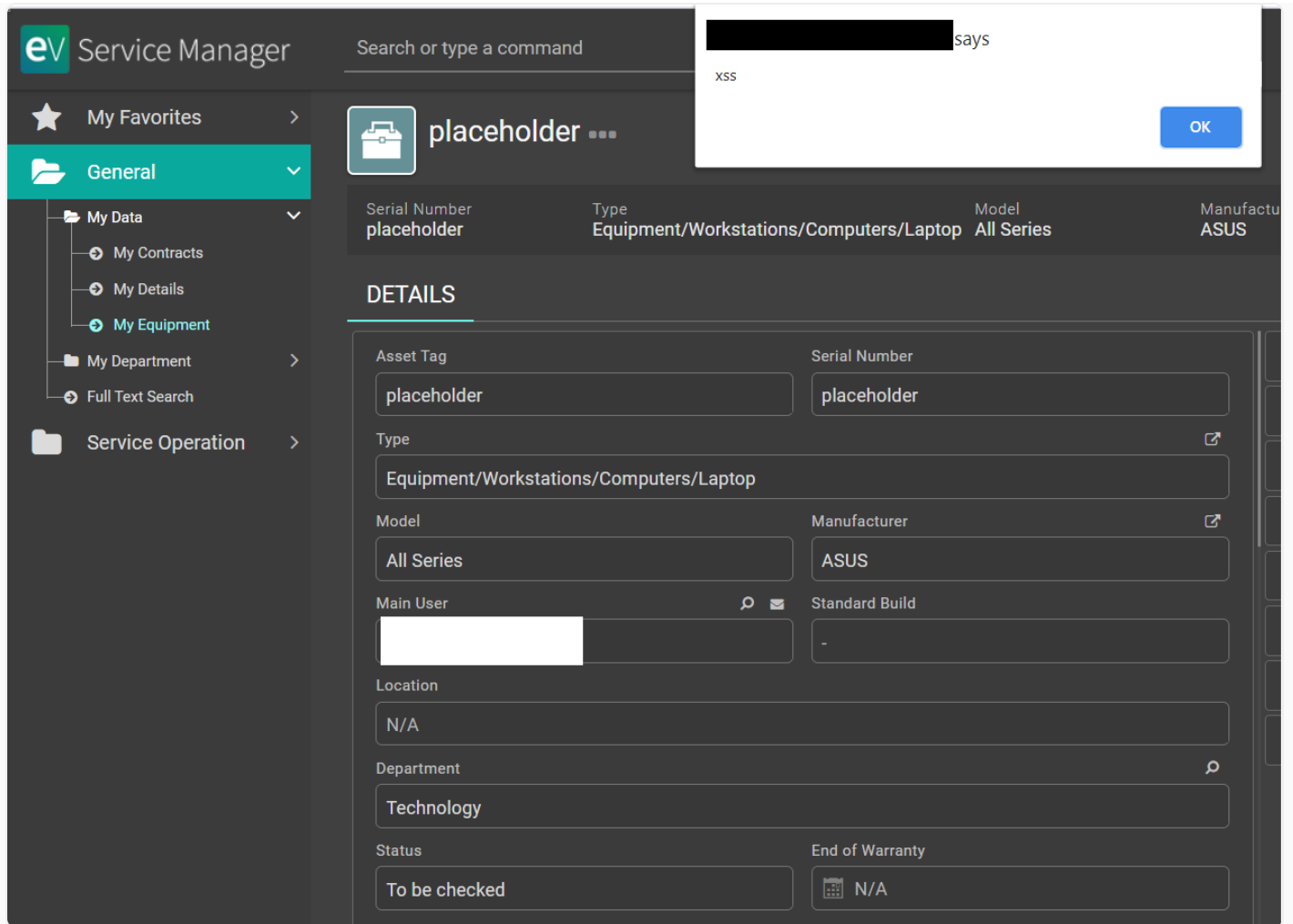
Location N/A

Finish Cancel

10 Records - 0 Selected

Status
To be checked
To be checked
To be checked
To be checked
To be checked
To be checked
To be checked
To be checked
Active
To be checked
To be checked

After submitting this new equipment entry, we incur into a case of stored cross-site scripting (XSS) where any other user — including administrators — that would consult the user’s equipment would have arbitrary JavaScript code being executed in their own browser. Please refer to the proceeding image where the `alert('xss')` code that was input in the “Note” field popped up an alert on the victim’s browser with the `xss` text in it. Notice that this JavaScript code can be replaced by more malicious code.



There is great variety of attacks based on XSS. These commonly include transmitting private data — such as cookies or other session information — to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable website.

Timeline

- **Dec 22, 2020** — Reached out to EasyVista to identify the best process to report a security vulnerability.
- **Feb 11, 2021** — After a second attempt, EasyVista suggested reaching out to their security e-mail address to report the issue.
- **Feb 11, 2021** — Vulnerability was reported to EasyVista's Security team.
- **May 7, 2021** — Contacted again EasyVista asking for updates.

- **May 7, 2021** — EasyVista Senior executive confirmed that the issue was successfully reproduced and fixed on the latest EasyVista Service Manager version.

Final notes

I wish to relay all my best wishes to EasyVista's security team for its straightforward approach to the reported security issue and to the security senior executive for its cordial relaying of the actions that were taken.

← All posts

@ArmyS1ck · github.com/armysick