

Explore the latest product updates and best practices at our hybrid Checkmk Conference #12 from June 16-18, 2026 – [Register here](#)



[back to website](#)

Werk #18989: Enforce permission checks on Quick Setup endpoints

Component	REST API								
Title	Enforce permission checks on Quick Setup endpoints								
Date	Mar 16, 2026								
Level	Trivial Change								
Class	Security Fix								
Compatibility	Compatible - no manual interaction needed								
Checkmk versions & editions	<table><tr><td>2.6.0b1</td><td>Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT</td></tr><tr><td>Not yet released</td><td></td></tr><tr><td>2.5.0b2</td><td>Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT</td></tr><tr><td>2.4.0p25</td><td>Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT</td></tr></table>	2.6.0b1	Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT	Not yet released		2.5.0b2	Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT	2.4.0p25	Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT
2.6.0b1	Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT								
Not yet released									
2.5.0b2	Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT								
2.4.0p25	Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT								

Before this fix any **authenticated users** could interact with the Quick Setup endpoints allowing them to edit the setups, fetch background job status and run quick setup actions.

Because the API previously lacked granular authorization checks, users with any level of permission could interact with the endpoints. By submitting crafted PUT and POST requests, it was possible to modify stage data and request the execution of quick setup actions. Furthermore, it was possible to read the state of the background jobs which could have led to the disclosure of sensitive information.

The endpoint logic has been updated to check whether the user is allowed to interact with a specific quick setup and if it has the required permission level to retrieve information and run actions on the setup.

This vulnerability was identified in a commissioned penetration test conducted by PS Positive Security GmbH.

This issue affects the all editions of Checkmk in the default configuration.

Affected Versions:

- 2.5.0
- 2.4.0

Vulnerability Management:

We have rated the issue with a CVSS Score of 5.3 Medium

(**CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N**) and assigned **CVE-2026-24096**.

To the list of all Werks

The Checkmk logo (formerly known as Check_MK) is a trademark of Checkmk GmbH. ©2026 Checkmk GmbH. All rights reserved.
[Update cookie preferences](#)