checkmk

back to website

Werk #19238: Fix cross-site scripting (XSS) vulnerability in HTML logs of Synthetic Monitoring test services

Component	User interface
Title	Fix cross-site scripting (XSS) vulnerability in HTML logs of Synthetic Monitoring test services
Date	Feb 19, 2026
Level	Trivial Change
Class	Security Fix
Compatibility	Compatible - no manual interaction needed

Checkmk versions & editions	
2.6.0b1 Not yet released	Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT
2.5.0b1	Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT
2.4.0p22	Checkmk Pro, Checkmk Ultimate, Checkmk Cloud, Checkmk Ultimate MT
2.3.0p43	Checkmk Pro, Checkmk Ultimate, Checkmk Ultimate MT

The Checkmk UI renders the HTML logs of Synthetic Monitoring test services. This functionality was vulnerable to cross-site scripting attacks via dedicated phishing links.

Details

The HTML logs are created on the Checkmk hosts were the synthetic tests are executed. A malicious actor with access such a host could attempt to inject malicious JavaScript code into these logs before they are transferred to the monitoring server. Therefore, when these logs are rendered via the standard workflow in the Checkmk UI, they are sandboxed insize an HTML `iframe`. However, after injecting the code, an attacker could create a phishing link to a page that renders the logs un-sandboxed. This page is not reachable from within the Checkmk UI, however, the link would look like a standard link to a Checkmk UI page. Example: `https://omd.site.example/site/check_mk/robotmk_suite_report.py?site=site01&host=winhost1.site01.example&service=my-synthetic-test&log_type=ok`.

As of this werk, such phishing links are not functional anymore.

We thank Lisa Gnedt (SBA Research) for reporting this issue.

Who's Affected

All editions of Checkmk are affected in the default configuration.

Affected Versions

- 2.4.0
- 2.3.0

Recommended Mitigations

Avoid clicking on phishing links such as the one mentioned above.

Vulnerability Management

We have rated the issue with a CVSS score of 7.3 High (`CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:H/VI:H/VA:H/SC:N/SI:L/SA:N`) and assigned `CVE-2025-64999`.

To the list of all Werks