Werk #18891: omd: Local privilege escalation when executing omd commands as root

Component	Site management
Title	omd: Local privilege escalation when executing omd commands as root
Date	Feb 25, 2026
Level	Major Change
Class	Security Fix
Compatibility	Incompatible - Manual interaction might be required

Checkmk versions & editions	
2.6.0b1 Not yet released	Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Ultimate MT
2.5.0b3	Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Ultimate MT
2.4.0p25	Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Ultimate MT
2.3.0p46	Checkmk Community, Checkmk Pro, Checkmk Ultimate, Checkmk Ultimate MT

A critical privilege escalation vulnerability existed when executing the administrative `omd` commands with root privileges. A **site user** could exploit this mechanism to escalate their privileges to root. This escalation could also be triggered automatically by standard system operations such as post update triggers.

Calling `omd` inside the site context is safe, as there is no path for the site user to escalate to root from within it.

Update instructions:

Do **not** use `omd` as root user to interact with your site until you have installed a patched version of Checkmk. Installing the update automatically sets the patched `omd` as your default system command. Running the standard package installation first, followed by this update procedure, is safe and will not trigger the vulnerability:

```
sudo omd stop
sudo omd update <site name>
```

Important Security Warning: `omd` always uses the version specified in the site directory. Therefore, you must update all sites and completely remove the vulnerable packages from your system in order to patch this vulnerability.

Question: What is the vulnerability and who is potentially affected?

Answer: This is a local privilege escalation. A user who already has access to modify the site context can place a malicious payload. When the `omd` command is subsequently executed by root, that payload is executed with root privileges, allowing the site user to become root.

The site user serves as an isolation layer between the host machine and the Checkmk instance. The following are some practical examples:

- **Shared Hosts:** If multiple sites share a server, a compromised site user can escalate to root, breaking isolation and taking over the entire host and all other sites.
- **Restricted Hosts:** If you deny root access to site administrators but allow tasks like uploading MKPs, they can exploit this to bypass your restrictions and gain full root access.
- **Dedicated Hosts:** If a single site runs alone on a server, the severity is lower. This is strictly a local privilege escalation for an already-compromised site user, not an external entry point.

Question: Is it still possible to interact with your site by performing actions as a site user?

Answer: Yes, `omd` is always safe to run as a site user. For example, this command is safe

```
su - <site name> -c "omd stop"
```

This command is safe even if `omd` has not been updated, yet.

Question: Is it sufficient to install the new version of the Checkmk package?

Answer: No, only the aforementioned update procedure is safe. This is because the version used by `omd` can be manipulated by the site user. As long as the vulnerable Checkmk version is present on the host, the system is not any safer. The old packages must be uninstalled. The patched `omd` executable can safely execute the following commands against a target site:

```
omd su <site name>
omd stop <site name>
omd start <site name>
omd update <site name>
omd rm <site name>
omd cleanup
```

```
omd version <site name>
omd setversion
```

The following commands are not safe to execute as a root user until old Checkmk versions have been uninstalled:

```
omd mv <site name> <new site name>
omd cp <site name> <new site name>
omd disable <site name>
omd enable <site name>
omd update-apache-config <site name>
omd restore <backup archive>
omd backup <site name>
omd init <site name>
omd create <site name>
```

Question: What are the alternatives if commands like `omd restore`, `omd backup`, `omd mv`, or `omd cp` trigger the vulnerability?

Answer: There is no direct workaround for `omd` commands that require root permissions on unpatched hosts. The old Checkmk packages must be uninstalled to use these commands safely again. `omd restore` and `omd backup` can be used safely by executing these commands as a site user. If you need to find the original site name from your backup archive, you can extract it like this:

```
tar -tzf <backup archive> | head -1 | cut -d/ -f1
```

Once you have the exact name, create the site and restore it from within the site context:

```
sudo omd create <exact_site_name>
sudo omd su <exact_site_name>
omd restore <backup archive>
```

Question: How can I verify whether the `omd`, which is currently in my path, is vulnerable?

Answer: You can verify this by checking for the new security flag file. The following snippet checks whichever `omd` executable is currently resolving in your active `$PATH`. Running this as **root** checks if your default system-wide `omd` command is vulnerable. Running it as a **site user** checks if that specific site's version is vulnerable.

```
VERSION=$(omd version -b)
if [ -f "/omd/versions/$VERSION/share/omd/security-werk-18891.flag" ]; th
  echo "System is PATCHED."
else
  echo "System is VULNERABLE."
fi
```

Question: How can I check which of my installed versions are affected?

Answer: You can check the status of all installed Checkmk versions on your host by running the following snippet:

```
for path in /omd/versions/*; do
  VERSION=$(basename "$path")
  if [ -f "$path/share/omd/security-werk-18891.flag" ]; then
    echo "$VERSION is PATCHED"
  else
    echo "$VERSION is VULNERABLE"
  fi
done
```

Affected Versions:

- 2.5.0 (beta)
- 2.4.0
- 2.3.0
- 2.2.0 (EOL, please upgrade to 2.3.0 or newer)

Vulnerability Management:

We have rated the issue with a CVSS Score of 9.3 Critical (`CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H`) and assigned `CVE-2025-39666`.

This issue was found during internal review.

To the list of all Werks