MENDER

Mender blog

CVE

CVE-2026-49009 & CVE-2026-33552 - Input sanitization and access control issues in Mender Server

Ethical hackers on our HackerOne bug bounty program recently discovered and disclosed security issues in Mender Server.

Ole Herman S. Elgesem | May 27, 2026 3 min read

These issues were fixed in Mender Server 4.1.1 and 4.0.2, and if you are using hosted Mender, it has already been patched for you.

CVE-2026-49009 - Improper input sanitization in Mender Server

A flaw in input sanitization was discovered in Mender Server 4.1.0, 4.0.1, and below, and fixed in 4.1.1 and 4.0.2. Thank you to j0xh-sec for discovering and responsibly disclosing this issue.

Description

Due to improper input sanitization in the endpoint for creating artifacts on the server (used from the UI or API), an attacker could include path traversal sequences like `../` in the request to access and modify files outside the intended directory. This enabled compromising the container for other users of the same API, allowing the attacker to inject arbitrary (malicious) code into the artifacts they are trying to create.

Impact

In order to exploit this, an attacker would need a user with permissions to access the specific API, and the victim would need to be using this specific feature. In the context of a multi-tenant system with many different organizations, like hosted Mender, it is guaranteed that some users are using the feature, and it is easy to sign up for an account with the needed permissions, and so the impact is severe in this case.

For an on-premise installation, this is different, since there are fewer users and it is usually not possible to just sign up for an account. Even if one got access to a user, it is significantly less likely that there are other users using the affected APIs that could be attacked.

If you are using cryptographically signed artifacts and have set up your Mender Client running on devices to verify signatures, the device would refuse to install any maliciously modified artifacts, and so you would not be affected.

Similarly, if you are not using the feature of creating Mender artifacts on the Server / via the API or UI, you are also not affected by this issue.

Remediation

If you are on one of the affected versions (Mender Server 4.1.0, 4.0.1, and earlier), we recommend upgrading. Upgrading to Mender Server 4.0.2 or 4.1.1 (or later versions) will fix the issue. Mender Server Enterprise and Mender Server Community (Open Source) are affected.

Our documentation has detailed upgrade instructions to help you:

https://docs.mender.io/server-installation/upgrading-from-previous-versions

CVE-2026-33552 - Improper access control in Device Group RBAC

A flaw in the role-based access control (RBAC) system was discovered in Mender Server 4.1.0, 4.0.1, and below, and fixed in 4.1.1 and 4.0.2. Thank you to Rajveer for discovering and responsibly disclosing this vulnerability.

Description

If an administrator tried to give *Read* access to some devices via one device group, and *Manage* access to other devices via another, the user would not end up with the intended access. When

combined, the user would end up with *Manage* access to both device groups, not just the one the administrator selected.

Impact

The system did not restrict access as appropriate, which means that if a user account, set up as described, was ever compromised by an attacker, it would have a higher level of access than necessary for some devices. It is a flaw in an important security feature, which is why we treat it seriously and inform our users about it, even though it can be seen as quite specific / narrow, and most users would probably find the impact of this very limited, if affected at all.

Remediation

If you are on one of the affected versions (Mender Server 4.1.0, 4.0.1, and earlier), we recommend upgrading. Upgrading to Mender Server 4.0.2 or 4.1.1 (or later versions) will fix the issue. RBAC is an enterprise-only feature, so only Mender Server Enterprise is affected (not Mender Server Community / Open Source).

Our documentation has detailed upgrade instructions to help you:

https://docs.mender.io/server-installation/upgrading-from-previous-versions

Contact

For help with upgrading or additional questions, please contact support at:

https://support.northern.tech

CVE

Recent articles

CVE

CVE-2025-67903 - Signature verification bypass in Mender Client

Security vulnerability enabling signature verification bypass in Mender Client version 5.0.0 to 5.0.3.

May 27, 2026 | 2 min read

Product News

Success with AI in MedTech depends on the software infrastructure beneath it

Explore how robust software infrastructure is essential for the success of AI in MedTech, ensuring compliance, security, and lifecycle sustainability in medical devices.

May 7, 2026 | 3 min read

View more articles →