Urgent: ThinLinc security issue

security, thinlinc

CendioOssman 1 8 April 2026 13:45

> **Release with fixes are now available: Click here**

A critical security issue has been discovered in the ThinLinc server that allows any user to impersonate any other user, including the root user. This issue affects all versions of ThinLinc.

Fixes for all supported versions of ThinLinc will be released at noon UTC 2026-04-22. Users running a version older than ThinLinc 4.15.0 should be prepared to not just apply the fix, but also to do an upgrade to a supported version.

There are no known mitigations for this issue. Users should be prepared to apply the fixed versions quickly once they are made available.

This issue was discovered by our partner Cosmikal S.L.

Update: See this thread for more discussion and details: **Questions about the critical ThinLinc security issue found on 04-08-2026**

3 Likes

Questions about the critical ThinLinc security issue found on 04-08-2026

CendioOssman 3 9 April 2026 14:26

As previously announced, a critical security vulnerability has been identified in the ThinLinc server. We understand that the period between the announcement and the availability of a fix creates challenges for your organization. This memo aims to provide additional context on our handling of this issue and guidance for your security monitoring.

1. Transparency on discovery and risk
The vulnerability was identified during a controlled penetration test conducted as part of our continuous security assurance activities, in collaboration with our partner Cosmikal S.L.

It is crucial to emphasize that:

- **Only users authorized** for the system can exploit this vulnerability. A user that cannot log in to the ThinLinc system cannot exploit this vulnerability.

- **No active exploitation** has been observed in the wild. There has been no indication that anyone outside Cendio and Cosmikal has details of this issue.

- Numerous earlier security reviews and penetration tests of ThinLinc have failed to discover this issue. It is therefore not likely to be easily found by a malicious actor.

- The disclosure follows a strict "**responsible disclosure**" protocol to ensure that no technical details are publicly known before a fix is ready for implementation.

2. Why we are following a strict release schedule

We have received requests for early access to patches or detailed mitigation steps. While we understand the urgency, our decision to adhere to the release date of **noon UTC 2026-04-22** is based on the following security principles:

- **Preventing reverse engineering**
  Any patch or technical details released prematurely can be analyzed to identify the exact nature of the flaw. This would effectively provide actionable insight for attackers to exploit ThinLinc systems that have not yet had the chance to update.

- Quality assurance
  Given the critical nature of the fix, it is undergoing rigorous testing to ensure system stability and that no secondary issues are introduced.

- Equity in protection
  Our responsibility is to protect the entire ThinLinc ecosystem simultaneously, preventing a window of risk for any part of our user base.

3. Guidance for monitoring and detection

While we cannot provide specific technical mitigations without revealing the vulnerability's mechanics, we recommend that security teams focus on the following:

- Ensure that access to the ThinLinc infrastructure is restricted to known and trusted users.

- Audit your system's logs for any anomalous patterns, specifically regarding root logins or unexpected privilege escalations.

4. Preparation for April 22nd

To ensure a smooth transition, we advise the following:

- Identify all ThinLinc instances in your environment. Any version older than **4.15.0** will require a full upgrade to a supported version to receive the fix.

- Pre-schedule a maintenance window at **noon UTC on April 22nd**. The security fixes will be released as a normal update and will be installed the same way as any other update to ThinLinc. Separate updates

will be released for every ThinLinc version that is currently supported.

Cendio takes the security of ThinLinc with the utmost seriousness. Our response follows industry best practices for coordinated vulnerability disclosure. We are committed to providing a stable, secure, and thoroughly tested solution that resolves this issue definitively.

We appreciate your patience as we work to secure your environment. If you have any questions or concerns, do not hesitate to contact us at **support@cendio.com**.

Sincerely,

Pierre Ossman, ThinLinc product owner, and the entire ThinLinc team

6 Likes

Related topics

Topic	Replies	Activity
Questions about the critical ThinLinc security issue found on 04-08-2026 security	4	9 April 2026
ThinLinc 4.15.1 through 4.20.1 security release thinlinc, security	1	23 April 2026
Server upgrade procedure for the 2026-04-08 security issue security	0	20 April 2026
Ruling out that the 2026-04-08 security issue was exploited security	0	22 April 2026
ThinLinc 4.16.0 released release, thinlinc	0	30 January 2024