Security Advisory: Update BTCPay Server to 2.4.2 Immediately

Posted in Announcements by BTCPay Server on 8/7/2026



Immediate action required

If you use **LND** and run a BTCPay Server version prior to 2.4.2, including a 2.4.2 release candidate, **update to version 2.4.2 now**.

If you use another Lightning implementation or do not use Lightning, you are not exposed to the LND credential risk. We still strongly encourage you to update.

What happened

The issue could allow an unauthenticated remote attacker to obtain `.macaroon` credential files for **LND, an implementation of the Lightning Network**. Those credentials could be used to take control of an LND node and move funds. The attacks we reviewed targeted only files with the `.macaroon` extension.

In our initial communications, out of an abundance of caution, we advised users to move funds out of their BTCPay Server on-chain wallets. After further review, we confirmed that only LND is impacted.

We have confirmed that attackers exploited this vulnerability. Users were affected and funds were stolen. We are not publishing technical details yet because operators still need time to update.

Who is impacted

Version	Status
All versions prior to 2.4.2, including 2.4.2 release candidates	❌ Contains the vulnerability. LND users must update immediately
2.4.2	✅ Fixed

- The vulnerability is present in every BTCPay Server version prior to 2.4.2, including the 2.4.2 release candidates.
- The risk of exposed `.macaroon` credentials and stolen funds applies specifically to deployments using LND. Users of other Lightning implementations and users who do not use Lightning do not need to update to address this LND credential risk, but we strongly encourage them to update BTCPay Server.
- BTCPay Server's on-chain wallets, including hot wallets, are not affected. Funds held in LND's own on-chain wallet are part of the affected LND node and may still be at risk.
- If you use LND, treat its credentials as potentially exposed and check the node for unauthorized activity.

How to mitigate the risk

1. Update to BTCPay Server 2.4.2 and LND 0.21.1

If you use LND, update immediately. All other users running a BTCPay Server version prior to 2.4.2 are strongly encouraged to update.

For a standard BTCPay Server installation, go to:

Server Settings → Maintenance → Update

To confirm that the update completed successfully, check that the admin footer shows BTCPay Server 2.4.2 and that your LND node is running version 0.21.1.

If your installation is managed another way, follow your usual update process.

If you use LND and cannot update right away, take the server offline until you can. Do not leave an affected LND deployment accessible from the internet.

2. Review your LND node activity

If you use LND:

- Check for payments you did not make.
- Look for unexpected channel closures or unfamiliar peers.
- Compare your on-chain and channel balances with your own records.
- Investigate any activity you do not recognize.

The update also upgrades LND to version 0.21.1 and automatically regenerates its macaroons. You can also rotate your macaroons manually.

If you expose your LND node through your own reverse proxy, Tor service, forwarded port, or another route outside BTCPay Server, rotate its credentials now. Updating BTCPay Server does not close access paths that you manage separately.

3. Be aware of temporary wallet connectivity changes

BTCPay Server domain or Tor onion address for now.

We made this change to protect LND nodes while the incident is ongoing. We plan to restore this option when it is safe to do so. If you depend on it, contact us and we will help you find another setup.

Summary

If you use LND and run **a BTCPay Server version prior to 2.4.2, update to 2.4.2 now**.

The vulnerability is present in all BTCPay Server versions prior to 2.4.2. Other Lightning implementations and deployments that do not use Lightning are not exposed to the LND credential risk and do not need to update for this specific issue, but we strongly encourage them to install the update. BTCPay Server's on-chain wallets, including hot wallets, are not affected.

If you use LND, check your node and balances for activity you do not recognize. If you cannot update now, take the server offline until you can.

We are deeply sorry to everyone affected by this incident. In the coming days, we will work on a full postmortem and share it when it is ready.

We would like to thank Craig Raw for responsibly disclosing the vulnerability and Team Red for working with us to analyze the exploit.

To report a security issue, email security@btcpayserver.org.

Last Updated: 11/2/2026, 2:22:16 PM

The BTCPay Server Project is proudly supported by these entities through the BTCPay Server Foundation.

Spiral OpenSats Tether HRF

LunaNode Wallet of Satoshi Coincards IVPN

Unbank

If you'd like to support the project, please visit the donation page.

Privacy Policy