



# CIRT.GY

Guyana National Computer Incident Response Team

## ADV2025\_451 TeamViewer Security Advisory (December 24<sup>th</sup>, 2025)

TeamViewer has published a security advisory highlighting vulnerabilities in the following products on December 11<sup>th</sup>, 2025. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- TeamViewer DEX Client – NomadBranch.exe – versions prior to 1E Client 25.11.0.29
- TeamViewer DEX Client – NomadBranch.exe – versions prior to 1E Client 25.9.0.46 - HF-PLTPKG-524 (Hotfix)
- TeamViewer DEX Client – NomadBranch.exe – versions prior to 1E Client 25.5.0.53 - HF-PLTPKG-526 (Hotfix)
- TeamViewer DEX Client – NomadBranch.exe – versions prior to 1E Client 24.5.0.69 - HF-PLTPKG-525 (Hotfix)
- TeamViewer DEX – multiple versions

For more information on these updates, you can follow these URLs:

- [Improper input validation in TeamViewer](#)
- [Command Injection and Privilege Escalation vulnerabilities in TeamViewer](#)
- [TeamViewer Trust Center](#)

The Guyana National CIRT recommends that users and administrators review these updates and apply them where necessary.

### References

- TeamViewer Security Advisory. (December 23, 2025). Retrieved from Canadian Centre for Cyber Security.  
<https://www.cyber.gc.ca/en/alerts-advisories/teamviewer-security-advisory-av25-861>
- Command Injection and Privilege Escalation vulnerabilities in TeamViewer. (December 11, 2025). Retrieved from TeamViewer.  
<https://www.teamviewer.com/latam/resources/trust-center/security-bulletins/tv-2025-1006/>