

Security Announcement

Statement on the AVERAT Malware Incident

iThome recently reported that cybersecurity firm Rapid7 had disclosed a Linux backdoor named AVERAT. The report mentioned characteristics associated with ShareTech device.

Based on the information currently made public by Rapid7, the report primarily analyzes how the malware operates within affected systems. **It does not explain how the attackers initially gained access to the devices, nor does it confirm that the incident was caused by a specific product vulnerability.**

ShareTech Mail Server can detect abnormal files and suspicious execution behavior within the system. When suspicious activity is detected, the system displays an alert in the management interface and can be configured to notify administrators by email for further review and action.

ShareTech will continue to conduct product security testing, vulnerability scanning, and threat analysis. If security issues requiring further action are confirmed, we will provide necessary updates.

We also recommend the following basic security practices for system administrators:

- Regularly check device system versions and security updates.
- Restrict external access to the device management interface.
- Use strong administrator passwords and change them regularly.
- Monitor the management interface for alerts about abnormal files or processes.
- If abnormal alerts or suspicious behavior are detected, contact ShareTech for assistance.

ShareTech Information Co., Ltd.

October 7, 2026

