ADVISORY FOR ICM SECTOR

Backdoor exploit against telecom systems

Original report published on: October 01, 2025

Executive Summary

Since April 2024, an Indonesian telecommunications entity has been compromised via a backdoor deployed by a threat actor that has been active since 2019 with a history of targeting telecommunications and government sectors. The backdoor is capable of harvesting user credentials on systems used for network-performance monitoring.

Based on its long-term deployment (from at least April 2024 to September 2025), the threat actor is likely to continue using this backdoor to compromise high-value credentials in future operations, particularly against Southeast Asia-based telecommunications entities.

Background

The threat actor targets privileged credential use for performance-monitoring by engineers or vendors to access critical network infrastructure. By replacing the legitimate *pam_unix.so* module with a malicious variant, the backdoor enables the attacker to harvest user credentials continuously for unauthorised access, capturing credentials in clear text and storing them in a file at */usr/share/awk/nullfile.awk*.

While credential harvesting activity was observed, the monitoring of Nokia Radio Access Network (RAN) traffic and the logging of traffic into packet-capture files were performed by a likely legitimate cron job running once per hour. This cron job invokes the *sudo* command during execution, which results in the periodic loading of *pam_unix.so*. The hourly execution of the cron job should not be interpreted as evidence that the backdoor was intended to maintain persistence.

A second variant of the backdoor stores captured credentials in a separate local file.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the backdoor identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A).
- Refer to the MITRE ATT&CK techniques in this advisory (Annex B):
  - Create, test and validate detection rules against the threat behaviours.
  - Validate and deny/disable processes, ports and protocols that have no business need.
- Monitor file creation events in Linux file path */usr/share/vim/.null* and */usr/share/awk/nullfile.awk.*
- Implement file integrity monitoring for critical system libraries, including *pam_unix.so* to identify any unauthorised changes or tampering.
- Enforce multi-factor authentication (MFA) for privileged access, regularly rotate passwords and enforce strong password policies for critical infrastructure systems to minimise the risk of credential compromise.
- Practice whitelisting for access to management plane and review access logs to detect unauthorised login attempts.
- Validate and add malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR) solutions.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

SHA256 Hash	Description
e5d14406c572b2bc6cb048ead718041c3f44b159078f97b4cb47cde26bff1fd6	Malware
e098f7a14eee6043708fdfaf2badd8fd12d8598bb2f2378caa36e0db07922571	Backdoor
4beed2c10155381b943ca15cbaf5ea23b69dd87eed18fc72482493e290a6c46f	Backdoor

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Persistence	T1574.006	Hijack Execution Flow: Dynamic Linker Hijacking
Defence Evasion	T1036.005	Masquerading: Match Legitimate Name or Location
Credential Access	T1003	OS Credential Dumping
	T1556.003	Modify Authentication Process: Pluggable Authentication Modules
Collection	T1074.001	Data Staged: Local Data Staging