

Hisense faces \$5 million ransom demand over alleged 19GB data theft

By Ernestas Naprys

Published: 2026-10-26 · Archived: 2026-10-30 02:00:54 UTC

Key takeaways

1. WhiteArmor claims it stole 19GB of Hisense data and demands \$5 million in Bitcoin.
2. The alleged data includes Malaysia and Singapore warranty records with customer details, invoices, contracts, and supplier information.
3. Hisense has not confirmed the breach, and the leaked sample was inaccessible at publication time.
4. A Cybernews researcher says verified claims would mainly expose customer personal information and warranty data.

Key Takeaways by nexos.ai, reviewed by Cybernews staff.

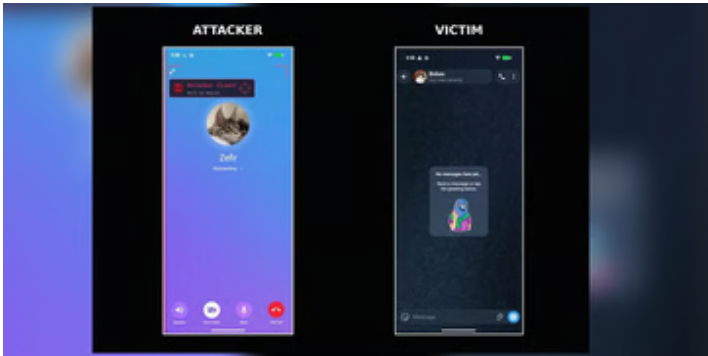
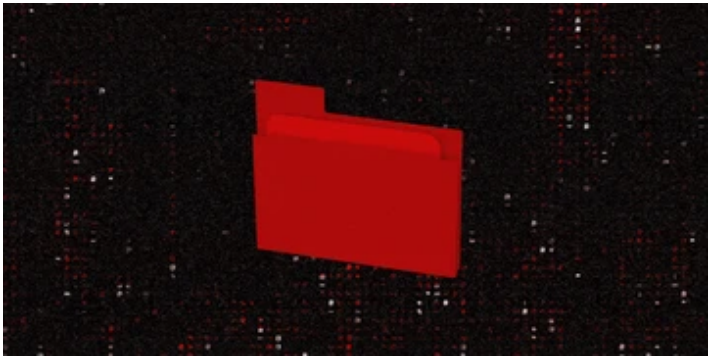
Hisense, a major Chinese electronics and home appliance manufacturer best known for TVs, has reportedly suffered a major data breach. A new ransomware gang, WhiteArmor, claims to have obtained 19GB of sensitive data and is demanding \$5 million in ransom. The breach hasn't been officially confirmed.

The threat actor has posted Hisense on its data leak site on the dark web, and the countdown timer leaves over 28 days for the company to react.

“Our demand is \$5,000,000 in BTC. Good luck,” the post by WhiteArmor ransomware operator reads.

The threat actor has already released a small data sample of 348KB and is threatening to release the full 19GB archive, currently sealed. However, at the time of writing, the sample was inaccessible – the hosting server was not responding.







The hackers claim to have obtained “Hisense’s entire GCRM production document store, the full warranty-claims archive for Malaysia/Singapore: customer names, phones, emails, ID numbers, 2,549 suppliers, hundreds of invoices, payments, contracts, RMA forms, claim evidence, plus their internal CRM app binary.”

Hisense

PUBLISHED 10/24/2026 09:33 PM 376 **SEALED**

28d 13:29:04

FILES RELEASE 11/24/2026 01:09 AM

Hisense is a Chinese multinational electronics and appliance manufacturer, founded in 1969, known globally for televisions and home appliances.

We hold Hisense’s entire GCRM production document store, the full warranty-claims archive for Malaysia/Singapore: customer names, phones, emails, ID numbers, 2,549 suppliers, hundreds of invoices, payments, contracts, RMA forms, claim evidence, plus their internal CRM app binary.

Our demand is \$5,000,000 in BTC. Good luck.

Contact: [REDACTED]

Session: [REDACTED]

Files are sealed. The attachments on this publication are withheld until the countdown above reaches zero. They will become available on this page automatically, no action needed.

WhiteArmor claims Hisense. Screenshot from a data leak site.

Some posts on X suggest that the attackers increased their demands from an initial \$500,000.

Cybernews has reached out to Hisense for comment and will include its response.

“If claims are true, the impact is limited to warranty claims for Malaysia/Singapore, together with customer details,” noted Aras Nazarovas, security researcher at Cybernews.

“It mostly affects the confidentiality of customers’ personally identifiable information, such as names, phone numbers, email addresses, and invoices.”

The attackers could potentially reverse-engineer the CRM app binary to target Hisense’s warranty claims processing systems with return fraud or to extract additional customer PII.

WhiteArmor is a new data-theft and extortion group that emerged only a few days ago – the first victim was claimed on October 21st, 2026. Currently, its data-leak site lists 6 victims.

The operator charges its affiliates only a 5% fee on successful ransom payments. DarkFeed, a cyber threat intelligence platform, reported that the threat actor is recruiting pentesters, web exploitation experts, and zero-day researchers. However, its claims remain unverified.

Source: <https://cybernews.com/security/ransomware-operator-claims-hisense-demands-5-million/>