# CVE Detail – CVE-2017-17704

A door-unlocking issue was discovered on Software House iStar Ultra devices through 6.5.2.20569 when used in conjunction with the IP-ACM Ethernet Door Module. The communications between the IP-ACM and the iStar Ultra is encrypted using a fixed AES key and IV. Each message is encrypted in CBC mode and restarts with the fixed IV, leading to replay attacks of entire messages. There is no authentication of messages beyond the use of the fixed AES key, so message forgery is also possible.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.37015

## CVSS Scoring

CVSS v3.0 Score: 7.4

Severity: HIGH

## Mapped CWE(s)

* CWE-330: Use of Insufficiently Random Values

## CAPEC(s)

* CAPEC-112: Brute Force
* CAPEC-485: Signature Spoofing by Key Recreation
* CAPEC-59: Session Credential Falsification through Prediction

## ATT&CK Techniques

* T1552.004: Private Keys
* T1110: Brute Force

## Used By (Actors/Tools)

* Machete (malware)
* Mafalda (malware)
* Hildegard (malware)
* Chaos (malware)
* FoggyWeb (malware)
* Caterpillar WebShell (malware)
* Pysa (malware)
* Troll Stealer (malware)
* Ebury (malware)
* Kinsing (malware)
* QakBot (malware)
* jRAT (malware)
* AADInternals (tool)
* Empire (tool)
* PoshC2 (tool)
* Mimikatz (tool)
* CrackMapExec (tool)
* Operation Wocao (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* TeamTNT (intrusion-set)
* APT28 (intrusion-set)
* HEXANE (intrusion-set)
* Volt Typhoon (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* APT39 (intrusion-set)
* APT38 (intrusion-set)
* Operation Dream Job (campaign)
* DarkVishnya (intrusion-set)
* APT41 (intrusion-set)
* Rocke (intrusion-set)
* Scattered Spider (intrusion-set)
* Agrius (intrusion-set)
* FIN5 (intrusion-set)

## Affected Products

* cpe:2.3:o:swhouse:istar\_ultra\_firmware:\*:\*:\*:\*:\*:\*:\*:\*