STA-22 · Mobile Threat Catalogue

Archived: 2026-04-06 02:09:33 UTC

Mobile Threat Catalogue

SIM Card Theft

Contribute

Threat Category: USIM / SIM / UICC security

ID: STA-22

Threat Description: A stolen SIM card allows an attacker to control the mobile number, open new cellular accounts using the victim's credentials, buy new phones as the victim, or steal the victim's identity altogether.[1]

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

AT&T SIM-Card Switch Scam [1]

4 Surprising Ways Your Identity Can Be Stolen [2]

CVE Examples

Not Applicable

Possible Countermeasures

Carriers

Carriers should be encouraged to strongly authenticate account holders before allowing account changes such as issuance of new SIM cards

References

1. AT&T SIM-Card Switch Scam, New York Department of State; www.dos.ny.gov/consumerprotection/scams/att-sim.html [accessed 8/23/16]. ↩ ↩[2]
2. G. Williams, "4 Surprising Ways Your Identity Can Be Stolen," U.S. News & World Report, 9 June 2015; http://money.usnews.com/money/personal-finance/articles/2015/06/09/4-surprising-ways-your-identity-can-be-stolen ↩
