SPC-11 · Mobile Threat Catalogue

Archived: 2026-04-05 22:43:53 UTC

Mobile Threat Catalogue

Vulnerable BIOS Installation

Contribute

Threat Category: Supply Chain

ID: SPC-11

Threat Description: An adversary with access to download and update system software installs a BIOS containing known vulnerabilities for future exploitation.[1]

Threat Origin

Supply Chain Attack Framework and Attack Patterns [1]

Exploit Examples

Not Applicable

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

System maintenance processes for highly sensitive components such as BIOS should require dual authentication to perform, reducing the likelihood a single adversary can introduce malware

Utilize systems with boot validation and attestation to verify that only genuine boot code is executed during system start-up, halting start-up if integrity verification for any component fails

References

1. J.F. Miller, “Supply Chain Attack Framework and Attack Patterns”, tech. report, MITRE, Dec. 2013; www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf ↩ ↩[2]