# SPC-12 · Mobile Threat Catalogue

Archived: 2026-04-06 03:34:38 UTC

## Mobile Threat Catalogue

## Corrupted Automated Installer

Contribute

**Threat Category:** Supply Chain

**ID:** SPC-12

**Threat Description:** An automated software update/patch downloader/installer can be corrupted to download malicious code and apply it to systems being sustained.[1]

**Threat Origin**

Supply Chain Attack Framework and Attack Patterns [1]

**Exploit Examples**

*Not Applicable*

**CVE Examples**

*Not Applicable*

**Possible Countermeasures**

**Enterprise**

Use fine-grained role-based access control mechanisms and user/service roles that reduce the potential that malicious installation or upgrade packages can introduce malware outside of files and directories allocated to the associated software

Scan systems with newly integrated or updated software components for indicators of compromise prior to production use

**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]

---