CVE-2020-0601 (Curveball) – Proof-of-Concept

Eine kurze Zusammenfassung und PoC-Überblick

Einleitung

CVE-2020-0601, auch bekannt als „Curveball“, bezeichnet eine Spoofing-Schwachstelle in der Windows CryptoAPI (Crypt32.dll). Durch fehlerhafte Validierung von ECC-Zertifikaten können Angreifer gefälschte Code-Signing-Zertifikate erstellen, mit denen Malware als vertrauenswürdig erscheint.

Hintergrund

Die Windows CryptoAPI prüft bei Signatur- und Zertifikats-Verification elliptische Kurven gemäß NIST P-256. Aufgrund einer fehlerhaften Implementierung kann ein Angreifer Parameter manipulieren, sodass gefälschte ECC-Zertifikate als gültig behandelt werden.

Schwachstelle

- **Betroffene Komponente:** Crypt32.dll (Windows 10, Server 2016/2019)
- **Art:** Unsichere Kurvenparameter-/Punktvalidierung
- **Ausnutzungsweg:** Erstellung eines manipulierten ECC-Zertifikats

Proof-of-Concept (PoC)

Für die Crypto-Challenge wird eine Python-Implementierung konzipiert und umgesetzt:

1. **Erzeugen eines manipulierten Zertifikats:** Modifikation von Kurvenparametern (z. B. Ordnung, Generator).
2. **Signaturerstellung:** Signieren einer Test-Binärdatei mit dem gefälschten Zertifikat.
3. **Verifikation:** Windows akzeptiert die Signatur und behandelt die Datei als von einer vertrauenswürdigen CA ausgestellt.

Auswirkungen

- *Vertrauensbruch:* Malware kann als legitim erscheinen.
- *Code-Ausführung:* Remote-Ausführung bösartiger Code-Signaturen.
- *Breite Angriffsfläche:* Alle Anwendungen, die CryptoAPI zur Zertifikatsprüfung nutzen.

Gegenmaßnahmen

- Installation des Microsoft-Sicherheitsupdates (z. B. KB4528760).
- Einsatz zusätzlicher Validierungstools (z. B. OpenSSL).
- Überwachung und Revocation verdächtiger Zertifikate.

Fazit

CVE-2020-0601 demonstriert, wie wichtig korrekte ECC-Parameterprüfung in Kryptobibliotheken ist. Die Python-PoC-Challenge vertieft das Verständnis für Spoofing-Angriffe auf Zertifikatsketten und sensibilisiert für sichere Implementierungen.