Pressinformation
3 februari 2026

Därför är fjärrstyrd kodkörning ett växande cyberhot

Fjärrstyrd kodkörning är en lika farlig som vanlig angreppsmetod vid cyberattacker. Genom att utnyttja mindre sårbarheter i programvara kan angriparen genomföra intrång och ta kontroll över kritiska system. Men det går att täppa till luckorna och minska sådana risker. Det börjar med goda rutiner för konfigurering och säkerhetsuppdatering, skriver Dan Schiappa, chef för produkter och tjänster på Arctic Wolf.

Förra året publicerades fler än digitala **48 000 sårbarheter**, en ökning på mer än 20 procent jämfört med 2024. En betydande del av dessa var allvarliga - mer än en tredjedel av alla sårbarheter bedömdes som “högrisk” eller “kritisk”.

Bland de sårbarheter som utgör de största hoten mot cybersäkerheten i företag har en typ hamnat i förgrunden: fjärrstyrd kodkörning (Remote Code Execution, RCE). En metod som ger angriparen möjlighet att på distans ta kontroll över en process eller enhet och köra sin egen kod.

Enligt säkerhetsforskare från Arctic Wolf svarade RCE för hälften av de 10 största sårbarheterna under 2024. Utvecklingen inom molntjänster och hybridarbete pekar mot att denna typ av sårbarhet både kommer att öka i antal och bli allvarligare över tid.

Vad är fjärrstyrd kodkörning?

Fjärrstyrd kodkörning (RCE – Remote Code Execution) innebär att programkod startas över Internet. Det ger en angripare möjlighet att ta kontroll över en enhet eller process på distans, utan att behöva befinna sig inom samma lokala nätverk som de angripna systemen.

En angripare som lyckas utnyttja en RCE-sårbarhet kan potentiellt skaffa sig fullständig kontroll över målsystemet, vilket öppnar för stöld av känsliga data, sabotage eller störningar av verksamheten eller att sätta igång ytterligare attacker.

Att det har blivit ett så populärt sätt att utföra cyberattacker förklaras av att det ger hotaktören direkt åtkomst utan att först tillskaffa sig inloggningsuppgifter genom nätfiske eller liknande metoder och utan att ha fysisk tillgång till målet för attacken.

Några stora RCE-attacker

WannaCry
Den kanske allra lömskaste av alla ransomware-varianter är WannaCry. Den visade sig först under 2017 och spreds genom att utnyttja en sårbarhet i Server Message Block Protocol (SMB). Denna sårbarhet gjorde det möjligt för en angripare att köra skadlig kod på oskyddade servrar, vilket öppnade för hackare att komma åt och kryptera värdefulla filer. WannaCry lyckades påverka över 200 000 Windows-datorer i 150 länder i attacker som har kopplats till nordkoreanska hotaktörer.

SolarWinds
Ett av de mest omfattande dataintrången 2020 genomfördes av den ryska säkerhetstjänsten SVR genom att utnyttja en sårbarhet i det populära IT-administrationsverktyget Orion från SolarWinds för att distribuera skadlig kod. Över 18 000 anslutna nätverk drabbades och hackarna skaffade sig tillgång till enorma mängder källkod, lösenord, finansiell information och användarnamn.

”Nollklicks”-attack mot Android

I november 2025 släppte Google en säkerhetsuppdatering av Android för att åtgärda en allvarlig sårbarhet (CVE-2025-48593) som potentiellt gav angripare möjlighet att kontrollera miljontals Android-mobiler och köra sin egen kod utan att användaren agerade genom att klicka, öppna eller installerade något. Denna typ av ”nollklick”-attacker är särskilt farliga eftersom offret kanske aldrig inser att deras enhet är drabbad. I en mobil miljö är RCE särskilt farligt eftersom smarta mobiler som regel rymmer mängder med känsliga data, bland annat personliga meddelanden, foton, inloggningsuppgifter och bankappar.

Att försvara sig mot fjärrstyrd kodkörning

Att lyckas förebygga RCE-attacker handlar mycket om goda säkerhetsrutiner, inte minst att omgående installera nya programuppdateringar och patchar. När sårbarheter upptäcks i programvara eller appar kommer deras utvecklare att släppa uppdateringar till användarna. Den som ser till att hålla sig uppdaterad med de senaste patcharna gör mycket för att minska risken för RCE.

En annan effektiv – och mer proaktiv – metod för att förhindra RCE är genom ett program för sårbarhetshantering som ständigt söker efter sårbarheter i din miljö och håller koll på ert patchschema.

Eftersom varje organisation har unika säkerhets- och verksamhetskrav som också kan förändras, bör målet med sårbarhetshantering inte vara att eliminera alla tänkbara sårbarheter, utan att tillämpa en riskbaserad strategi som minskar risken över tid.

Mer information

- Diskutera med Arctic Wolf på Facebook, X, LinkedIn och YouTube.
- Besök arcticwolf.com och ta reda på mer om våra lösningar för operativ IT-säkerhet.

Mediakontakt
Fredrik Pallin
Digital PR
fredrik@digitalpr.dk

Om Arctic Wolf

Arctic Wolf är en global ledare inom operativ cybersäkerhet som hjälper företag att minska riskerna med cyberattacker. Arctic Wolfs molnbaserade säkerhetsplattform Aurora förenar kraften hos artificiell intelligens med världsledande säkerhetsexpertis för att erbjuda övervakning, motåtgärder och riskhantering dygnet runt. Vi får säkerhet att fungera!
www.arcticwolf.com