AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësitë kritike të RCE në Apache MINA

Data: 28/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Dy dobësi kritike—CVE-2026-41635 dhe CVE-2026-41409—janë identifikuar në Apache MINA, një framework aplikacionesh rrjeti e bazuar në Java e përdorur gjerësisht.

Informacione Teknike

Dy dobësi kritike - CVE-2026-41635 dhe CVE-2026-41409 - janë identifikuar në Apache MINA, një framework aplikacionesh rrjeti e bazuar në Java e përdorur gjerësisht. Të dy dobësitë kanë një rezultat CVSS prej 9.8 (Kritik) dhe mundësojnë Ekzekutimin e Kodit në Distancë (RCE) nëpërmjet mekanizmave të pasigurt të deserializimit.

Detajet e dobësisë:
1. CVE-2026-41635 – Anashkalimi i Listës së Lejimeve në Deserializim
• Ashpërsia: Kritike (CVSS 9.8)
• Lloji: Validim i gabuar i hyrjes / Gabim Logjik
• Shkaku root:

Në AbstractIoBuffer.resolveClass(), degë të caktuara ekzekutimi (p.sh., klasa statike ose lloje primitive) nuk zbatojnë kontrollet e listës së lejuar të emrit të klasës.
• Ndikimi:
Sulmuesit mund të krijojnë ngarkesa të serializuara që anashkalojnë validimin.
Lejon ekzekutimin e klasave arbitrare që çojnë në RCE.

• Vektori i Sulmit:
o I largët, i paautorizuar (në varësi të ekspozimit të aplikacionit).

• Problemi Kryesor:
o Zbatim jokonsistent i filtrit acceptMatchers.

2. CVE-2026-41409 – Zbatim i Vonë i Listës së Lejimeve (Rregullim i Paplotë)
• Ashpërsia: Kritike (CVSS 9.8)
• Lloji: Deserializim i Pa sigurt / Renditje e gabuar e Inicializimit
• Shkaku root:
o Validimi i listës së lejimeve zbatohet pas ngarkimit të klasës.
o Java ekzekuton inicializues statikë pas ngarkimit të klasës, para validimit.

• Ndikimi:
o Kodi keqdashës i ngulitur në blloqet statike ekzekutohet para kontrolleve të sigurisë.
o Çon në RCE para-validimit.

• Vektori i Sulmit:

o Shfrytëzim i largët nëpërmjet objekteve të serializuara të krijuara.

• Problemi Kryesor:
o Korrigjim i paplotë i dobësisë së mëparshme (CVE-2024-52046).

Versionet e prekura
• 2.2.x: 2.2.0 → 2.2.5
• 2.1.x: 2.1.0 → 2.1.10
• 2.0.x: 2.0.0 → 2.0.27

Versione të përditësuar
• 2.0.28
• 2.1.11
• 2.2.6

Rekomandime

AKSK rekomandon të përditësoni Apache MINA në versionet e patch-uara.