



**AUTORITETI KOMBËTAR  
PËR SIGURINË KIBERNETIKE**

**Dobësi me ashpërsi të lartë në Juniper Networks Junos OS dhe  
Junos OS Evolution**

Data: 24/04/2026  
Version: 1.0

## Përmbajtja

Përmbledhje Ekzekutive .....	2
Informacione Teknike .....	2
Rekomandime .....	2

## Përmbledhje Ekzekutive

---

Një dobësi me rëndësi të lartë në Juniper Networks Junos OS dhe Junos OS Evolved. E meta i lejon një sulmuesi të paautorizuar të ndërpresë operacionet e rrjetit duke rivendosur seancat BGP duke përdorur paketa të krijuara posaçërisht, duke çuar në një gjendje Mohimi të Shërbimit (DoS).

## Informacione Teknike

---

Detajet e dobësisë

CVE-2026-33797 – Validimi i gabuar i hyrjes që çon në rivendosjen e sesionit BGP (DoS)

• Ashpërsia: E lartë | CVSS v3.1: 7.4

• Një dobësi e validimit të gabuar të hyrjes në Junos OS dhe Junos OS Evolved lejon një sulmues të paautorizuar në një rrjet ngjitur të dërgojë një paketë BGP të krijuar posaçërisht, por të vlefshme brenda një sesioni BGP të krijuar tashmë. Shfrytëzimi i suksesshëm shkakton rivendosjen e sesionit BGP të synuar, duke rezultuar në një gjendje Mohimi të Shërbimit (DoS). Shfrytëzimi i vazhdueshëm mund të mbajë ndërprerjen, duke ndikuar në stabilitetin e rrugëzimit. Dobësia ndikon si në implementimet e eBGP ashtu edhe në iBGP në mjediset IPv4 dhe IPv6.

Versionet e Prekura

• Junos OS: versionet 25.2 para 25.2R2

• Junos OS Evolved: versionet 25.2-EVO para 25.2R2-EVO

Versionet e përditësuara

• Junos OS: 25.2R2, 25.4R1 dhe versione më të vona

• Junos OS Evolved: 25.2R2-EVO, 25.4R1-EVO dhe versione më të vona

## Rekomandime

---

AKSK rekomandon përditësimin e versioneve të prekura në versionet e rregulluara ose më të fundit të publikuara nga Juniper Networks.