

Pažeidžiamumo identifikatorius: CS0019

Atradimo data: 2010-03-07

Produktas: Kaspersky Anti-Virus for Windows Workstations 6.0.4.1212

Pažeidžiamumo tipas: blogai nustatytos failų sistemos teisės, privilegijų pasikėlimas

Pavojus:  (Aukštas)

Atakos realizavimas: lokalus

Kataloge „%ALLUSERSPROFILE%\Kaspersky Lab\AVP60MP4\Data“ yra saugomi laikini antivirusinės programos atnaujinimui skirti failai. „Data“ katalogui ir visiems jo pakatalogiams bei failams yra nustatytos įrašymo teisės, kurios suteikia galimybę visiems sistemos vartotojams kurti ir modifikuoti failus. Modifikavus „rollback.ini“ failą, įmanoma priverti antivirusinę programą perrašyti pasirinktą sistemos failą, jeigu tai bus sistemos tarnybos failas – gauti „SYSTEM“ privilegijas.

Demonstracija: <http://www.critical.lt/blogs/show/kaspersky-antivirusines-programos-isnaudojimas-privilegiju-gavimui/>

Sprendimas: laukti gamintojo pataisos, nustatyti administravimo slaptažodį