NewsRoom

4/3/07 Network World (Pg. Unavail. Online)
2007 WLNR 6743637

Network World
Copyright © 2007 Network World - All Rights Reserved

April 3, 2007

Deceiving Cisco's NAC
* Fooling Cisco's NAC is possible but complicated

Tim Greene

Cisco's NAC can be fooled into thinking non-compliant PCs actually meet the security posture NAC is designed to enforce, according to security experts reporting at the Black Hat conference in Europe.

That means Cisco's NAC could admit non-compliant PCs to networks because it can't tell that it is being lied to.

So if a PC tells Cisco's NAC policy server what it needs to hear - that its personal firewall settings are proper; and its antivirus is updated to a certain point; and its operating system is patched to a set level - it will admit the device. Cisco's NAC will not know that the data is phony.

Cisco's response is that such deceptions are possible, but Cisco NAC still authenticates users. So while Cisco NAC might admit unqualified machines to networks, it can only be duped by someone who can also successfully authenticate the machines to the NAC policy server.

Carrying out this type of ruse is complicated. For instance, a person has to know the proper posture information to pass up to Cisco's NAC policy server in order to successfully fool it. If the PCs antivirus software must have been updated to a certain signature release from a certain vendor, the person behind the deception has to know that information in order to succeed.

The Black Hat presentation addresses only Cisco NAC, not other NAC endpoint-checking schemes, and they may be similarly vulnerable.

Security experts say one point to take a way from this is that as a matter of course it is ill advised for devices to report on their own state for just this reason.

Endpoint checking has always had its shortcomings. Even if the device doesn't lie to the policy server, the information it assesses can't prove that the device is safe to admit to the network. It can only indicate that it is less likely to infect the network.

The demonstration of this weakness makes endpoint checking in the Cisco environment less useful.

---- Index References ----

Company: CISCO SYSTEMS INC

News Subject: (Major Corporations (1MA93))

Industry: (Security Software (1SE53); I.T. (1IT96); Networking (1NE45); I.T. in Security (1IT64); I.T. Vertical Markets (1IT38); Firewalls (1FI23); Networking Security (1NE79))

Language: EN

Other Indexing: (BLACK HAT; CISCO; CISCO NAC; FOOLING; NAC; PC) (Cisco; Deceiving Cisco)

Word Count: 380

End of Document

© 2024 Thomson Reuters. No claim to original U.S. Government Works.

NewsRoom