1400 - Attacking Autonomic Networks

Saturday at 14:00 in 101 Track

45 minutes | Demo, Exploit

Omar Eissa*Security Analyst, ERNW GmbH*

Autonomic systems are smart systems which do not need any human management or intervention. Cisco is one of the first companies to deploy the technology in which the routers are just "Plug and Play" with no need for configuration. All that is needed is 5 commands to build fully automated network. It is already supported in pretty much all of the recent software images for enterprise level and carrier grade routers/switches.

This is the bright side of the technology. On the other hand, the configuration is hidden and the interfaces are inaccessible. The protocol is proprietary and there is no mechanism to know what is running within your network.

In this talk, we will have a quick overview on Cisco's Autonomic Network Architecture, then I will reverse-engineer the proprietary protocol through its multiple phases. Finally, multiple vulnerabilities (overall 5) will be presented, one of which allows to crash systems remotely by knowing their IPv6 address.

Omar Eissa

Omar Eissa is a security Analyst working for ERNW. His interests are network security and reverse-engineering. He is a professional Cisco engineer with various years of experience in enterprise and ISPs networks. He has given talks and workshops at various telco events and conferences like Troopers17 and Black Hat USA 2017.

#defcon25/by_track/101/saturday #defcon25/By_Day/_saturday