Black Nurse Attack

Security Updates for Black Nurse Attack

Summary

Cautela Labs is aware of a recently discovered attack that can crash a company's firewall and routers. This attack works like a DDoS attack using ICMP packets to "ping" your network and cause a denial of service.

Detailed Information

This attack leverages ICMP type 3 "unreachable" messages, using ICMP Type 3 Code 3 "port unreachable". TDC researchers define low bandwidth as a DoS attack of 15 to 18 Mbps. "This is to achieve the volume of packets needed, which is around 40 to 50K packets per second. It does not matter if you have a 1 Gbit/s internet connection. The impact we see on different firewalls is typically high CPU loads. When an attack is ongoing, users from the LAN site will no longer be able to send/receive traffic to/from the internet. All firewalls we have seen recover when the attack stops." (http://www.networkworld.com/article/3140925/security/blacknurse-attack-1-laptop-can-dos-some-firewalls-bring-down-big-servers.html)

Affected systems per researchers

- Cisco ASA 5506, 5515, 5525 (default settings)
- Cisco ASA 5550 (legacy) and 5515-X (latest generation)
- Cisco Router 897 (can be mitigated)
- SonicWall (misconfiguration can be changed and mitigated)
- Some unverified Palo Alto
- Zyxel NWA3560-N (wireless attack from LAN side)
- Zyxel Zywall USG50

Corrective Action

Different kinds of mitigations can be implemented to minimize the impact of the attack. On firewalls and internet facing equipment, a list of trusted sources for which ICMP is allowed could be configured. Disabling ICMP Type 3 Code 3 on the WAN interface can mitigate this attack.

Anti-DDoS mitigation

Use of professional anti-DDoS solutions from ISPs can mitigate the BlackNurse attack as well as other forms of DDoS attacks.

Additional References

(Network World, Nov 13, 2016 8:25 AM PT). BlackNurse attack: 1 laptop can DoS some firewalls, bring down big servers. Retrieved from http://www.networkworld.com/article/3140925/security/blacknurse-attack-1-laptop-can-dos-some-firewalls-bring-down-big-servers.html

Lenny Hansson. Per Høgh. Bjarne Bachmann. Kenneth B. Jørgensen. Dennis Rand (2016). The BlackNurse Attack. Retrieved from http://soc.tdc.dk/blacknurse/blacknurse.pdf