‘BlackNurse’ Firewall Bug Heightens DDoS Risk

A bug in several popular firewalls could allow large websites to be taken offline by attackers wielding minimal resources, according to security researchers.

The ‘BlackNurse’’attack would allow a successful denial-of-service (DoS) attack against firewall products from Cisco and Zyxel to be launched from a single laptop, according to researchers at the Security Operations Centre of Danish telecommunications company TDC.

Single-laptop attack

Palo Alto Networks firewalls can be affected in specific, non-default settings, Palo Alto acknowledged, and Sonicwall products can be attacked “if misconfigured”, according to an advisory from Netresec.

Denial-of-service attacks more typically involve traffic flooded from large numbers of source systems, often controlled by malicious botnets.

In this case attackers could take down the firewall by sending traffic amounting to only 18 Mbps, well within what could be managed by an ordinary laptop on an average Internet connection, TDC said.

“We had expected that professional firewall equipment would be able to handle the attack,” the researchers wrote in an advisory.

While the attack is carried out, the network protected by the firewall is unable to send or receive data from the Internet, they said.

Large networks at risk

“Even though traffic speed and packets per second were very low, this attack could keep our customers’ operations down,” they stated. “This even applied to customers with large Internet uplinks and large enterprise firewalls in place.”

The firewalls tested recovered once the attack stopped.

The attack involves repeatedly sending a particular type of control message to the firewall – an ICMP Type 3 Code 3 “port unreachable” message, according to TDC.

In most cases the firewall can be configured to block all ICMP traffic, neutralising the issue, but TDC said Cisco ASA series 55xx units are still vulnerable even with this workaround in place.

The firm’s advisory includes a list of suggested mitigations, and Palo Alto and SANS Internet Storm Centre also published information on workarounds.

The government recently established a National Cyber Security Centre under the auspices of GCHQ, acknowledging that online systems are increasingly essential to national security.

UPDATED 16/11/2016: The original article stated SonicWall firewalls were affected, however this is only the case if they are “misconfigured.” Sonicwall has told *TechWeekEurope* its products are not impacted.

“SonicWall engineering received TDC’s report on BlackNurse in September 2016, and worked directly with Lenny Hanson from TDC, one of the researchers who wrote the report,” a spokesperson said.

“SonicWall testing showed that with normal ICMP flood protection on, the SonicWALL firewall was not vulnerable.”