CERT-EU Security Advisory 2016-141

BlackNurse ICMP DoS Attacks

November 14, 2016 — v1.0

History:

- *14/11/2016 — v1.0: Initial publication*

Summary

TDC-SOC-CERT the CERT from TDC A/S, a Danish telecommunications company, observed and started analyzing a number of Denial-of-Service (DoS) attacks based on the ICMP protocol. As a result, in one of their analyses [1], they have noticed that one of the attacks was based on the ICMP protocol. This attack was not based on pure flooding of the internet connection but based on Internet Control Message Protocol (ICMP) Type 3 Code 3 packets. This attack was named **BlackNurse**.

The importance of this attack relies upon the fact that even though traffic speed and packets per second were very low, this attack could keep network operations down. This even applies to networks with large internet uplinks and large enterprise firewalls in place.

Technical Details

BlackNurse is an ICMP attack that sends a low volume of ICMP Type 3 (*Destination Unreachable*) Code 3 (*Port Unreachable*) requests to the target. BlackNurse is a form of Denial-of-Service (DoS) attack and the TDC report claims that it has the potential to disrupt the target organization's operations.

BlackNurse harnesses data based on the ICMP protocol, which routers and other networking devices use to send and receive error messages. By sending a special type of ICMP packets – specifically Type 3 ICMP packets with a code of 3 – attackers can quickly strain the CPUs of certain types of firewalls. After reaching a threshold of 15 to 18 Mbps, the targeted firewalls drop so many packets that the server behind the device effectively drops off the Internet. The TDC-SOC-CERT devised an attack that required only a single laptop to deliver BlackNurse volumes of 180 Mbps [2].

Is not recommended to block all Type 3 ICMP messages. In particular Type 3 Code 4 (*Fragmentation Needed and Don't Fragment was Set*) messages are required for path MTU discovery, which many modern operating systems use. So, in order to keep Path MTU discovery working our recommendation is to either rate-limit incoming ICMP traffic on an upstream router or deny incoming ICMP type 3 packets except for ICMP type 3 code 4 packets (*Fragmentation Needed*), since they are used for path MTU discovery.

Vulnerable Systems

Devices currently (14/11/2016) verified by TDC to be vulnerable to the BlackNurse attack:

- Cisco ASA 5506, 5515, 5525, 5540 (default settings)
- Cisco ASA 5550 (Legacy) and 5515-X (latest generation)
- Cisco Router 897 (unless rate-limited)
- Palo Alto (unless ICMP Flood DoS protection is activated, see advisory from Palo Alto [3])
- SonicWall (if misconfigured)
- Zyxel NWA3560-N (wireless attack from LAN Side)
- Zyxel Zywall USG50

Solutions

Block Type 3 ICMP messages with the exclusion of Type 3 Code 4 (*Fragmentation Needed and Don't Fragment was Set*) if needed.

Different kinds of mitigations can be implemented to minimize the impact of the attack. On firewalls and other kinds of equipment, a list of trusted sources for which ICMP is allowed could be configured. Use of professional anti-DDoS solutions from ISPs can mitigate the BlackNurse attack, as well as other forms of DDoS attacks. Implementing a flood protection, rate-limit, or DOS protection feature if available in the vulnerable appliance is strongly advisable.

For the detection of BlackNurse attacks TDC-SOC-CERT have released the following SNORT IDS rules:

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"TDC-SOC - Possible BlackNurse attack from
  external source "; itype:3; icode:3; detection_filter:track by_dst, count 250, seconds 1;
  reference:url, soc.tdc.dk/blacknurse/blacknurse.pdf; metadata:TDC-SOC-CERT,18032016;
  priority:3; sid:88000012; rev:1;)

alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"TDC-SOC - Possible BlackNurse attack from
  internal source"; itype:3; icode:3; detection_filter:track by_dst, count 250, seconds 1;
  reference:url, soc.tdc.dk/blacknurse/blacknurse.pdf; metadata:TDC-SOC-CERT,18032016;
  priority:3; sid:88000013; rev:1;)
```

A simple PoC for the BlackNurse attack [4] and a dedicated website [5], are available.

References

[1] http://soc.tdc.dk/blacknurse/blacknurse.pdf

[2] http://www.netresec.com/?page=Blog&month=2016-11&post=BlackNurse-Denial-ofService-Attack

[3] http://researchcenter.paloaltonetworks.com/2016/11/note-customers-regardingblacknurse-report

[4] https://github.com/jedisct1/blacknurse

[5] http://www.blacknurse.dk