Advanced Notification of BlackNurse Denial-of-Service attack

Security Advisory AE-Advisory 16-038

Criticality Critical

Advisory Released On 14 November 2016

Impact

Unavailability of network resources.

Solution

Refer to the “Solution” section below

Affected Devices (As of 14th November 2016)

- Cisco ASA 5506, 5515, 5525 (default settings)
- Cisco ASA 5550 (Legacy) and 5515-X (latest generation)
- Cisco Router 897

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a new denial-of-service attack that has surfaced within the past two days. It goes by the name “BlackNurse” attack and is able to bring large servers offline with very limited bandwidth and effort because it is fairly different than the other well-known denial-of-service attacks. It is still unknown which devices are affected and which are not, however, most of the very well-known network devices have been affected by this attack. Further details are explained in the “Threat Details” section below.

Threat Details

BlackNurse is a low bandwidth ICMP attack that uses Type 3 Code 3 packets. Once a user allows ICMP Type 3 Code 3 to outside interfaces, the BlackNurse attack becomes very effective even at a low bandwidth rate (15-18 Mbit/s). Once a network device (e.g: firewall) is impacted, the CPU load increases drastically and while the attack is ongoing, users from the same local area network will no longer be able to send and/or receive traffic to/or from the Internet. Once the attack stops, the firewall recovers and everything goes back to normal again.

To know if your network devices are vulnerable to this attack (**Please note that aeCERT does not recommend attempting this test on a live/production environment)**, you will have to allow ICMP on the WAN interface of your firewall and test with Hping3 which is merely a ping tool with custom TCP/IP packet sending capabilities. You will then need to attempt to attack the WAN interface from the outside by using Hping3 with one of the following commands:

```
hping3 -1 -C 3 -K 3 -i u20 <target ip>
hping3 -1 -C 3 -K 3 --flood <target ip>
```

A reasonable sized laptop can produce approximately the exact bandwidth needed to reproduce this attack successfully.

Since this attack is fairly new, it is still unknown as to what devices are affected and so, the “Affected Devices” list above covers all of the devices affected up until the date of this advisory’s release (14th November 2016).

Solution

If you have found that your network devices are vulnerable to the BlackNurse attack then below are a few workarounds:

1. Deny ICMP Type 3 messages sent to the WAN interface of Cisco ASA firewalls. However, before doing so, Cisco has warned that the disabling of Type 3 messages will also disable Path MTU discovery. So, to keep it working, it is recommended 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 since they are used for Path MTU discovery.

2. Another alternative is to upgrade the Cisco ASA to a higher end one with multiple CPU cores as the BlackNurse attack seems to not be as effective on multi-core ASAs.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae