Volume 2016-42-1

Cisco ASA IKE Buffer Overflow

CVE-2016-1287

Summary

We want to alert our customers to a critical vulnerability affecting Cisco ASA Software Internet Key Exchange (IKE) version 1 and IKE version 2. The vulnerability in the affected code area could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code using a specially crafted UDP packet.

Detailed Information

A critical remote code execution vulnerability has been discovered in Cisco's Adaptive Security Appliance (ASA) software which would allow a remote, unauthenticated attacker to gain full control of the system. This vulnerability can only be exploited using traffic directed to an affected system which has been configured to terminate IKEv1 or IKEv2 VPN connections, which are accessible from the Internet when deployed. This vulnerability can be triggered by IPv4 and IPv6 traffic using a single specially crafted UDP packet directed to port 500 or 4500.

Corrective Action

There are no workarounds that address this vulnerability. Cisco has provided software updates which address the vulnerability and it is recommended to upgrade as soon as possible.

Affected Cisco ASA Software running on the following products may be affected by this vulnerability:

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower 9300 ASA Security Module
- Cisco ISA 3000 Industrial Security Appliance

Run the following command, the system is vulnerable if a crypto map is returned;

```
ciscoasa# show running-config crypto map | include interface
```

Additional References

Cisco Security Advisory - 20160210
Exodus Intel - Technical Write-up
CVE-2016-1287
SANS port 500 traffic