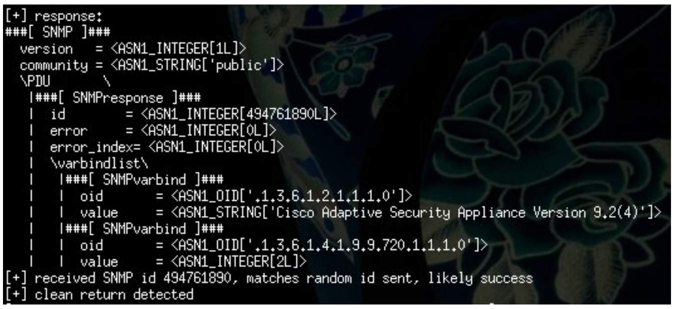
Cisco starts releasing security patches for a critical flaw affecting Adaptive Security Appliance (ASA) flaws-- one involving an exploit linked to the US National Security Agency (NSA).



```
[+] response:
###[ SNMP ]###
  version   = <ASN1_INTEGER[1L]>
  community = <ASN1_STRING['public']>
  \PDU       \
   |###[ SNMPresponse ]###
   |  id        = <ASN1_INTEGER[494761890L]>
   |  error     = <ASN1_INTEGER[0L]>
   |  error_index= <ASN1_INTEGER[0L]>
   |  \varbindlist\
   |   |###[ SNMPvarbind ]###
   |   |  oid       = <ASN1_OID['.1.3.6.1.2.1.1.1.0']>
   |   |  value     = <ASN1_STRING['Cisco Adaptive Security Appliance Version 9.2(4)']>
   |   |###[ SNMPvarbind ]###
   |   |  oid       = <ASN1_OID['.1.3.6.1.4.1.9.9.720.1.1.1.0']>
   |   |  value     = <ASN1_INTEGER[2L]>
[+] received SNMP id 494761890, matches random id sent, likely success
[+] clean return detected
```

Dubbed ExtraBacon, the exploit was recently discovered in networking hardware from Cisco and Fortinet. It is the work of a group called Shadow Brokers, who claims to have stolen "cyber weapons" from the Equation, a group believed to be an elite NSA hacking unit through its use of a 16-character string listed in an NSA manual leaked by Edward Snowden. ExtraBacon is actually just part of the toolset obtained by Shadow Brokers, and the full leaked set is currently available on auction for a million bitcoins.

The exploit affects versions 8.4(4) and earlier of ASA software, although it can be modified to work on newer versions. It involves a buffer overflow vulnerability in the Simple Network Management Protocol (SNMP) implementation, and allows attackers to remotely execute rogue code in affected devices through traffic sent to the SNMP interface.

Patched software is available for different ASA branches, namely 9.1.7(9), 9.5(3) and 9.6.1(11). Cisco suggests devices using 8.x amd 7.x branch ASA software should be migrated to 9.7.7(9), while patches for versions 9.0, 9.2, 9.3 and 9.4 should be available as 9.0.4(40), 9.2.4(14), 9.3.3(10) and 9.4.3(8).

Mind, ExtraBacon is not the only ASA exploit found in the Shadow Brokers leak-- there is also EpicBanana, an exploit of a vulnerability Cisco insists was patched back in 2011 with version 8.4(3), although the company still has an advisory covering the flaw.

A third exploit comes in legacy Cisco PIX firewalls. Named BenignCertain, it affects versions 6.x and earlier of the PIX software, and as such it is advised users should update to version 7.0 and later.

Go Cisco Adaptive Security Appliance SNMP Remote Code Execution Vulnerability