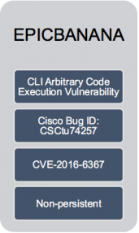
## 

## Cisco Adaptive Security Appliance

## EPICBANANA

A privilege escalation exploit against Cisco Adaptive Security Appliance (ASA) and Cisco Private Internet eXchange (PIX) devices. Exploitation takes advantage of default Cisco credentials (password: cisco). Affects ASA versions 711, 712, 721, 722, 723, 724, 80432, 804, 805, 822, 823, 824, 825, 832 and PIX version 711,712,722,723,724, 804.

<https://musalbas.com/2016/08/16/equation-group-firewall-operations-catalogue.html>



The EPICBANANA exploit leverages the vulnerability CVE-2016-6367 and could allow an authenticated attacker to create a Denial of Service (DoS) condition or potentially execute arbitrary code. An attacker could exploit this vulnerability by invoking certain invalid commands in an affected device. The attacker must know the telnet or SSH password in order to successfully exploit an affected device.

<https://blogs.cisco.com/security/shadow-brokers>

*“The attacker must source the attack from an IP address that is allowed by the SSH or telnet commands in the Cisco ASA. This is why it is a best practice to only allow SSH or telnet connections from trusted sources and on certain interfaces only (such as the management interface).”*

## Vulnerable Products

Cisco ASA Software releases earlier than 8.4(3) are vulnerable. An attacker must have local access and be authenticated to exploit this vulnerability.

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 PIX Firewalls
* Cisco Firewall Services Module (FWSM)

Vulnerability

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli>