Million CISCO ASA Firewalls potentially vulnerable to attacks

February 11, 2016 By Pierluigi Paganini

A flaw in Cisco ASA Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code.

It's a bad period for IT manufacturers, recently the security community has discovered serious and anomalous vulnerabilities affecting popular products like Juniper equipment and Fortinet Forti OS firewalls.

Now, it is now the turn of Cisco, the product line Cisco ASA firewall, a family of devices that is offered for sale as an appliance, blades or even virtual systems.

The Cisco ASA Adaptive Security Appliance is an IP router that acts as an application-aware firewall, network antivirus, intrusion prevention system, and virtual private network (VPN) server.

deployed.

Security experts David Barksdale, Jordan Gruskovnjak, and Alex Wheeler of Exodus Intelligence have discovered a critical buffer overflow vulnerability (CVE-2016-1287) that received a CVSS (Common Vulnerability Scoring System) score of 10.

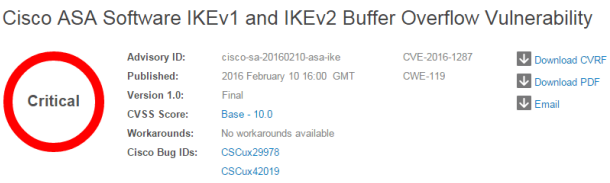
"The algorithm for re-assembling IKE payloads fragmented with the Cisco fragmentation protocol contains a bounds-checking flaw that allows a heap buffer to be overflowed with attacker-controlled data. A sequence of payloads with carefully chosen parameters causes a buffer of insufficient size to be allocated in the heap which is then overflowed when fragment payloads are copied into the buffer. Attackers can use this vulnerability to execute arbitrary code on affected devices." is the summary published by Exodus Intel.

It is quite easy for an attacker to exploit the vulnerability in CISCO ASA by sending crafted UDP packets to the vulnerable system. An exploit could allow the attacker to obtain full control of the system

The impact is serious considering that over a million of CISCO ASA firewall has been already deployed worldwide.

"A vulnerability in the Internet Key Exchange (IKE) version 1 (v1) and IKE version 2 (v2) code of Cisco ASA Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code." states the Advisory published by CISCO.

"The vulnerability is due to a buffer overflow in the affected code area. An attacker could exploit this vulnerability by sending crafted UDP packets to the affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system or to cause a reload of the affected system."



Which are the affected devices?

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

> “
>
> Cisco ASA 5500 Seri
> Adaptive Security Ap
> Cisco ASA 5500-X Se
> Next-Generation Fire
> Cisco ASA Services M
> for Cisco Catalyst 6
> Series Switches and
> 7600 Series Routers
> Cisco ASA 1000V Clo
> Firewall
> Cisco Adaptive Secu
> Virtual Appliance (A
> Cisco Firepower 9300
> Security Module
> Cisco ISA 3000 Indus
> Security Appliance

If you have one of them patch it as soon as possible.

Pierluigi Paganini

(Security Affairs – Cisco ASA firewall, hacking)

buffer overflow | CISCO ASA Firewall | CVE-2016-1287 | Hacking

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
Poseidon Group, a single actor behind a long series of attacks

NEXT ARTICLE
Once again identity thieves use stolen SSNs in IRS attack

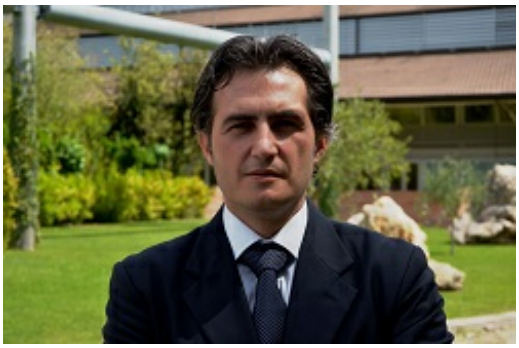
YOU MIGHT ALSO LIKE

Man charged of Laundering $19.6 Million earned with PBX system hacking

February 14, 2016 By Pierluigi Paganini

The IPT ruled that GCHQ spies can legally hack any electronic devices

February 13, 2016 By Pierluigi Paganini



- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group,

he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top