

[TOOL] Cisco Torch – Mass Cisco Vulnerability Scanner

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0064.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/15/05

To: list@securiteam.com

Date: 15 Feb 2005 14:51:20 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Cisco Torch – Mass Cisco Vulnerability Scanner

SUMMARY

DETAILS

In the process of writing "Hacking Exposed Cisco Networks" Andrew got dissatisfied with the Cisco scanners currently available and decided to do our own. Some code (telnet fingerprint scan and several entries in the telnet fingerprinting database) are borrowed from Hackbot – thank you guys for writing an excellent tool. The main feature that makes Cisco-torch different from similar tools is the extensive use of forking to launch multiple scanning processes on the background for maximum scanning efficiency. Also, it uses several methods of application layer fingerprinting simultaneously, if needed. Andrew wanted something fast to discover remote Cisco hosts running Telnet, SSH, Web, NTP and SNMP services and launch dictionary attacks against the services discovered.

It should be fast enough to crunch through a large company or a small country. In addition, the tool finds classical, but still relevant Cisco IOS HTTP Auth and Cisco Catalyst 3500 XL Remote Arbitrary Command Execution Vulnerabilities. Andrew could (and we will) add more vulnerabilities to check for, but mind it we are not interested in DoS,

Securiteam: [TOOL] Cisco Torch – Mass Cisco Vulnerability Scanner

only enable.

By the way, this seems to be the only tool that does Cisco fingerprinting via NTP, spare for the NTP Nessus plugin. Application layer fingerprinting performed against several services on the host is fast and reliable. And if none of these services are running, it is unlikely that you will manage to get into that Cisco box anyway, at least when you aren't on the same LAN.

As to the dictionary/bruteforcing attacks, we could've done them faster, but we didn't parallel the attacks to get maximum efficiency when attacking large networks (kind of paralleling it by IP's, rather than processes).

ADDITIONAL INFORMATION

The information has been provided by <mailto:andrew@arhont.com> Andrew A. Vladimirov.

To keep updated with the tool visit the project's homepage at:
<www.arhont.com/cisco-torch-0.2b.tar.bz2>
www.arhont.com/cisco-torch-0.2b.tar.bz2

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.