

Securiteam: [NEWS] Vulnerability in the TCP Protocol Allows RST Spoofing (Cisco Advisory)

[NEWS] Vulnerability in the TCP Protocol Allows RST Spoofing (Cisco Advisory)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0088.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/22/04

To: list@securiteam.com

Date: 22 Apr 2004 18:48:30 +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>

Vulnerability in the TCP Protocol Allows RST Spoofing (Cisco Advisory)

SUMMARY

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly.

DETAILS

Vulnerable Systems:

- * All Cisco products which contain a TCP stack are susceptible to this vulnerability.
- * A full list can be found at the original advisories linked below.

Immune Systems:

- * Cisco VPN 3000 Series Concentrators
- * Cisco Firewall Services Module for Cisco Catalyst 6500 Series and Cisco 7600 Series (FWSM)

Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for

Securiteam: [NEWS] Vulnerability in the TCP Protocol Allows RST Spoofing (Cisco Advisory)

example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection that must be considered. This attack vector is only applicable to the sessions that are terminating on a device (such as a router, switch, or computer), and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, the attack vector does not directly compromise data integrity or confidentiality.

TCP is the transport layer protocol designed to provide connection-oriented reliable delivery of a data stream. To accomplish this, TCP uses a mixture of flags to indicate state and sequence numbers to identify the order in which the packets are to be reassembled. TCP also provides a number, called an acknowledgement number that is used to indicate the sequence number of the next packet expected. The packets are reassembled by the receiving TCP implementation only if their sequence numbers fall within a range of the acknowledgement number (called a "window"). The acknowledgement number is not used in a packet with the reset (RST) flag set because a reset does not expect a packet in return. The full specification of the TCP protocol can be found at <http://www.ietf.org/rfc/rfc0793.txt>. According to the RFC793 specification, it is possible to reset an established TCP connection by sending a packet with the RST or synchronize (SYN) flag set. In order for this to occur, the 4-tuple must be known or guessed (source and destination IP address and ports) together with a sequence number. However, the sequence number does not have to be an exact match; it is sufficient to fall within the advertised window. This significantly decreases the effort required by an adversary: The larger the window, the easier it is to reset the connection. While source and destination IP addresses may be relatively easy to determine, the source TCP port must be guessed. The destination TCP port is usually known for all standard services (for example, 23 for Telnet, 80 for HTTP). Many operating systems (OSs) use predictable ephemeral ports for known services with a predictable increment (the next port which will be used for a subsequent connection). These values, while constant for a particular OS and protocol, do vary from one OS release to another.

Here is an example of a normal termination of a TCP session:

```
Host(1) Host(2)
||
||
| ACK ack=1001, window=5000 |
|<-----|
||

Host(1) is closing the session

| RST seq=1001 |
|----->|
||
```

Securiteam: [NEWS] Vulnerability in the TCP Protocol Allows RST Spoofing (Cisco Advisory)

Host(2) is closing the session

In addition, the following scenario is also permitted:

```
Host(1) Host(2)
||
||
| ACK ack=1001, window=5000 |
|<-----|
||
```

Host(1) is closing the session

```
| RST seq=4321 |
|----->|
||
```

Host(2) is closing the session

Note how the RST packet was able to terminate the session although the sequence number was not the next expected one (which is 1001). It was sufficient for the sequence number to fall within the advertised "window". In this example, Host(2) was accepting sequence numbers from 1001 to 6001 and 4321 is clearly within the acceptable range.

As a general rule, all protocols where a TCP connection stays established for longer than one minute should be considered exposed.

Impact:

The impact is different for each specific protocol. While, in the majority of cases, a TCP connection will be automatically re-established, in some specific protocols a second order of consequences may have a larger impact than tearing down the connection itself. The Cisco PSIRT has analyzed multiple TCP-based protocols, as they are used within our offering, and we believe that this vulnerability does not have a significant impact on them. We will present our analysis for a few protocols that have the potential for higher impact due to the long-lived connections.

Voice signaling H.225, H.245 (part of H.323 suite):

H.225 and H.245 protocols are used in voice signaling. Their purpose is to negotiate parameters for content transfer (voice or video). The established sessions persist for the duration of a call. Any call in progress is terminated when the signaling session is broken. A new signaling session will be established immediately for the new call, but terminated calls cannot be re-established.

Each call from an IP telephone or softphone will result in the creation of a single signaling session. Terminating that signaling session affects

Securiteam: [NEWS] Vulnerability in the TCP Protocol Allows RST Spoofing (Cisco Advisory)

only a single user. It is possible that a single signaling session is responsible for multiple calls, but that setup is used deeper within the Service Provider's network. Determining all necessary parameters for mounting an attack is deemed a non-trivial task if the network is designed according to the current best practices.

Network Storage (iSCSI, FCIP):

Network Storage products use two TCP-based protocols: SCSI over IP (iSCSI) and Fiber Channel over IP (FCIP).

* SCSI over IP (iSCSI)

iSCSI is used in a client/server environment. The client is your computer and it is only the client that initiates a connection. This connection is not shared with any other users. A separate session is established for each virtual device used. Terminating the session will not have any adverse consequences if people are using current drivers from Microsoft for Windows and from Cisco for Linux. These drivers will re-establish the session and continue transfer from the point where it was disconnected.

Drivers from other vendors may behave differently.

The user may notice that access to a virtual device is slightly slower than usual.

* Fiber Channel over IP (FCIP)

FCIP is a peer-to-peer protocol. It is used for mirroring data between switches. Each peer can initiate the session. Switches can, and should be in practice, configured in a mesh. Bringing one link down will cause traffic to be re-routed over other link(s). If an adversary can manage to terminate the session multiple times in a row, the user's application may terminate with a "Device unreachable" or similar error message. This does not have any influence on the switch itself and the user can retry the operation.

The user may notice that access to a virtual device is slightly slower than usual. An occasional error message is possible.

Transport Layer Security/Secure Socket Layer (TLS/SSL)

Since this vulnerability operates on a TCP layer, encryption does not provide any protection. SSL/TLS connections can be used to encapsulate various kinds of traffic and these sessions can be long lived. A successful exploitation does not impact confidentiality of the data. An encrypted session can be attacked either on the originating or terminating host or on the firewalls in front of them (if they exist).

Workarounds:

The effectiveness of any workaround is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround is the most appropriate for use in the intended network before it is deployed.

Securiteam: [NEWS] Vulnerability in the TCP Protocol Allows RST Spoofing (Cisco Advisory)

There are no workarounds available to mitigate the effects of this vulnerability.

It is possible to mitigate the exposure on this vulnerability by applying anti-spoofing measures on the edge of the network.

By enabling Unicast Reverse Path Forwarding (uRPF), all spoofed packets will be dropped at the first device. To enable uRPF, use the following commands.

```
router(config)#ip cef
router(config)#ip verify unicast reverse-path
```

Please consult

<http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d41.html>
<http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d41.html>
and <<ftp://ftp-eng.cisco.com/cons/isp/security/URPF-ISP.pdf>>

<<ftp://ftp-eng.cisco.com/cons/isp/security/URPF-ISP.pdf>> for further descriptions of how uRPF works and how to configure it in various scenarios. This is especially important if you are using asymmetric routing.

Access control lists (ACLs) should also be deployed as close to the edge as possible. Unlike uRPF, you must specify the exact IP range that is permitted. Specifying which addresses should be blocked is not the optimal solution because it tends to be harder to maintain.

Caution: In order for anti-spoofing measures to be effective, they must be deployed at least one hop away from the devices which are being protected. Ideally, they will be deployed at the network edge.

Solution:

Install vendor patch. List of available software fixes is available at the full advisory linked below.

Exploitation and Public Announcements:

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

The exploitation of the vulnerability with packets having RST flag set (reset packets) was discovered by Paul (Tony) Watson of OSVDB.org. The extension of the attack vector to packets with SYN flag set and the vendors cooperating on the resolution of this issue discovered data injection.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@cisco.com>> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>>
<<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>>

Securiteam: [NEWS] Vulnerability in the TCP Protocol Allows RST Spoofing (Cisco Advisory)

And:

<<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>>

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>

=====

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.