Allegati alla lezione "VULNERABILITA' APPLICATIVE E WEB HACKING"

 1

-- Security Alert Consensus --
Number 048 (02.48)
Thursday, December 5, 2002
Created for you by
Network Computing and the SANS Institute
Powered by Neohapsis

***** {02.48.013} NApps - NetScreen predictable TCP ISN**

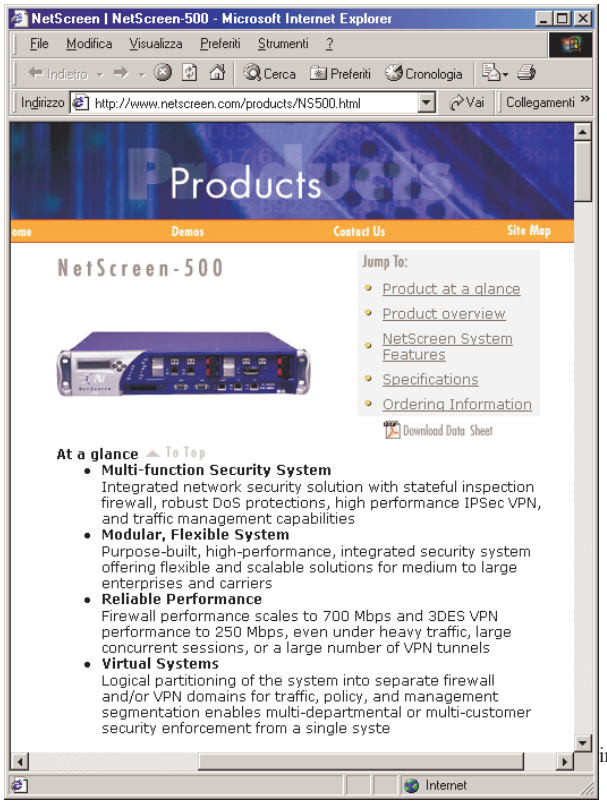
A NetScreen advisory indicates the TCP ISN random number generation in devices using ScreenOS 4.0 and prior is predictable, potentially leading to hijack/spoofed TCP sessions.

This vulnerability is confirmed and fixed in ScreenOS version 4.0.1.

Source: VulnWatch
http://archives.neohapsis.com/archives/vulnwatch/2002-q4/0095.html

 2

Consideriamo questo annuncio di vulnerabilita' apparso recentemente come caso di studio.



NetScreen ScreenOS

NetScreen ScreenOS firmware powers the entire system.
At its core is a custom-designed, real time operating system

- stateful inspection firewall

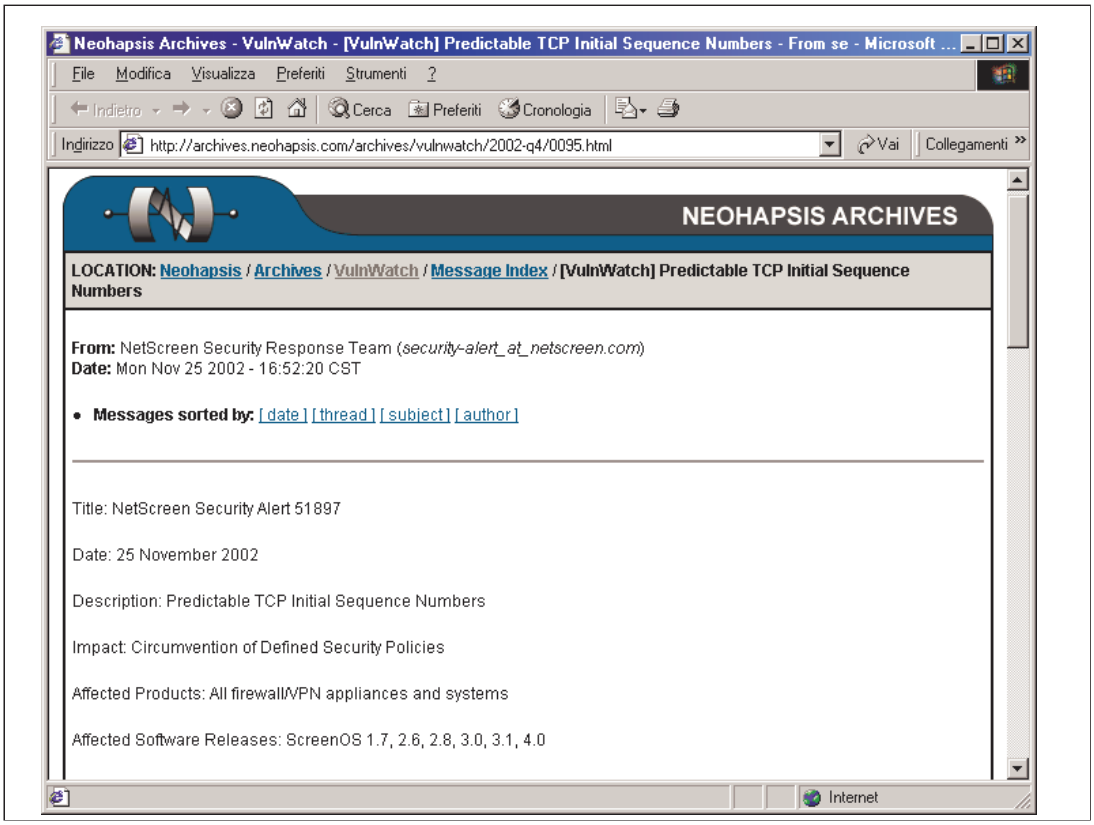
- IPSec VPN gateway

- traffic management capabilities for maximizing limited bandwidth

ini 3

La vulnerabilita' discussa va intesa come semplice esempio didattico.

Per nessun motivo va interpretata come giudizio di merito sul prodotto in oggetto.



Accediamo alla pagina indicata nell'annuncio della vulnerabilita' che contiene la descrizione i dettagli tecnici associati.

http://archives.neohapsis.com/archives/vulnwatch/2002-q4/0095.html

The vulnerability is exploitable on TCP connections to and from the NetScreen device itself.
...
The algorithms used to select TCP ISNs in affected versions of ScreenOS 2.6 and earlier are most predictable, thus the risks associated with this vulnerability are higher for devices running these versions of ScreenOS.
...
Recommended Actions:

Any or all of

(1) Install one of the maintenance releases indicated below.

(2) Upgrade to ScreenOS 4.0.1.

(3) Only permit protocols that make interception and modification detectable (IPSec, SSH, SSL, etc.) to traverse the firewall.

(3) ...

(4) Follow standard good security practices regarding configuration of the NetScreen device and communication to and from it that makes interception and modification detectable, if not altogether preventable. Examples include using IPSec tunnels or SSH to the device for administrative access to the CLI, MD5 authentication to protect BGP sessions, strong authentication for access control, and so on.


```
**********************************************************************
                  SANS Critical Vulnerability Analysis
November 25, 2002                                        Vol. 1. No. 18
**********************************************************************

Table of Contents:
- -----------------
Widely Deployed Software
(1) CRITICAL: IE/IIS Microsoft Data Access Components (MDAC) Buffer
    Overflow
(2) HIGH: iPlanet Compromise via Cross-Site Scripting in Admin
    Log Files
(3) HIGH: IE "Shortcut" ActiveX Control Restriction Bypass
(4) MODERATE: Cisco PIX HTTP Authentication Buffer Overflow

Other Software
(5) HIGH: LibHTTPD Malformed POST Buffer Overflow
(6) HIGH: Light HTTPd Malformed URI Buffer Overflow
(7) HIGH: Zeroo HTTP Server Malformed URI Buffer Overflow
(8) HIGH: TFTPD32 TFTP Server for Windows Multiple Vulnerabilities
```


Vediamo un altro esempio di annuncio di vulnerabilita' molto recente.

Notare che:

- molte riguardano Buffer Overflow (gia' visto in precedente lezione);
- una riguarda un servizio di File Transfer (TFTP) per piattaforma Windows;
- una riguarda un firewall (Cisco PIX);
- una riguarda un "active content" di applicazioni Web (ActiveX);
- una riguarda il caso di Cross-Site Scripting (di cui si parlera' in dettaglio nel capitolo "Vulnerabilita' di Applicazioni Web".

Oltre a questo, e' da osservare come le vulnerabilita' siano associate ad un grado di rischio: CRITICO/ALTO/MODERATO/BASSO

Vediamo secondo quali criteri il SANS valuta le vulnerabilita'.

****
Critical Vulnerability Analysis Scale Ratings

In ranking vulnerabilities several factors are taken into account, such as:

- **Is this a server or client compromise? At what privilege level?**
- **Is the affected product widely deployed?**
- **Is the problem found in default configurations/installations?**
- **Are the affected assets high value (e.g. databases, e-commerce servers)?**
- **Is the network infrastructure affected (DNS, routers, firewalls)?**
- **Is exploit code publicly available?**
- **Are technical vulnerability details available?**
- **How difficult is it to exploit the vulnerability?**
- **Does the attacker need to lure victims to a hostile server?**

Based on the answers to these questions, vulnerabilities are ranked as Critical, High, Moderate, or Low.

Fattori considerati:

- e' un intrusione lato server o lato client? Con quale livello di accesso?

- il prodotto corrispondente e' ampiamente diffuso?

- il problema riscontrato riguarda configurazioni/installazioni di default?

- i componenti coinvolti sono di valore/criticita' elevata? (es. database, server di e-commerce, etc.)

- l'infrastruttura di rete viene coinvolta? (es, DNS, router, firewall)

- esiste ed e' disponibile pubblicamente un codice che automatizza l'intrusione?

- sono disponibili tutti i dettagli tecnici?

- quanto e' difficili sfruttare la vulnerabilita'?

- e' necessario che l'intrusore induca la vittima ad accedere ad un server sotto il suo controllo?

CRITICAL vulnerabilities are those where essentially all planets align in favor of the attacker. These vulnerabilities typically affect default installations of very widely deployed software, result in root compromise of servers or infrastructure devices, and the information required for exploitation (such as example exploit code) is widely available to attackers. Further, exploitation is usually straightforward, in the sense that the attacker does not need any special knowledge about individual victims, and does not need to lure a target user into performing any special functions.

HIGH vulnerabilities are usually issues that have the potential to become CRITICAL, but have one or a few mitigating factors that make exploitation less attractive to attackers. For example, vulnerabilities that have many CRITICAL characteristics but are difficult to exploit, do not result in elevated privileges, or have a minimally sized victim pool are usually rated HIGH. Note that HIGH vulnerabilities where the mitigating factor arises from a lack of technical exploit details will become CRITICAL if these details are later made available. Thus, the paranoid administrator will want to treat such HIGH vulnerabilities as CRITICAL, if it is assumed that attackers always possess the necessary exploit information.

CRITICO - vulnerabilita' che:

- riguardano installazioni di default di pacchetti software ampiamente diffusi;
- provocano intrusioni con accessi di root a server o dispositivi;
- sono ampiamente documentate ed esiste codice facilmente reperibile per automatizzarne l'attacco;
- non richiedono competenze tecniche specialistiche.

ALTO - vulnerabilita' che hanno il potenziale per essere considerate critiche ma per le quali esiste una o piu' fattori che ne mitigano la pericolosita', quali:

- difficolta' tecniche;
- acquisizione di privilegi utente (non root);
- riguardano pacchetti software non estremamente diffusi;

etc.

MODERATE vulnerabilities are those where the scales are slightly tipped in favor of the potential victim. Denial of service vulnerabilities are typically rated MODERATE, since they do not result in compromise of a target. Exploits that require an attacker to reside on the same local network as a victim, only affect nonstandard configurations or obscure applications, require the attacker to social engineer individual victims, or where exploitation only provides very limited access are likely to be rated MODERATE.

LOW vulnerabilities usually do not affect most administrators, and exploitation is largely unattractive to attackers. Often these issues require the attacker to already have some level of access to a target (e.g. be able to execute arbitrary SQL queries, or be able to pop mail from a mail server), require elaborate specialized attack scenarios, and only result in limited damage to a target. Alternatively, a LOW ranking may be applied when there is not enough information to fully assess the implications of a vulnerability. For example, vendors often imply that exploitation of a buffer overflow will only result in a denial of service. However, many times such flaws are later shown to allow for execution of attacker-supplied code. In these cases, the issues are reported in order to alert security professionals to the potential for deeper problems, but are ranked as LOW due to the element of speculation.

MODERATO - vulnerabilita' per le quali esistono molte contromisure efficaci a disposizione, molte limitazioni tecniche oppure che hanno impatto non distruttivo:

- denial-of-service;
- richiedono che l'attaccante acceda alla stessa rete locale della vittima;
- riguardano configurazioni non standard o applicazioni scarsamente usate;
- consentono intrusioni con livello di accesso minimale.

BASSO - vulnerabilita' dirette a un pubblico estremamente limitato e di scarso interesse per un intrusore oppure nei casi in cui le informazioni tecniche a riguardo siano scarse e non del tutto affidabili.