

Adressat: Kunde
Versanddatum: 05.08.2003

scip ID: 221
Klasse: Denial of Service (DoS)

Securitylücke:

Linux Kernel 2.4.x NFS XDR decode_fh Denial of Service

Vulnerability Stufe:

kritisch

Datum Publizierung:

29.07.2003

Davon betroffen:

Linux Kernel 2.4.x bis 2.4.21

Advisory:

<http://www.securityfocus.com/archive/1/330888>

Patch:

<http://www.kernel.org/>

Erklärung:

Linux ist ein freies, UNIX-ähnliches Betriebssystem, das der General Public License (GPL) unterliegt. Es wurde 1991 vom Finnen Linus Torvalds ins Leben gerufen. Heute gilt es als grösster Konkurrent zum kommerziellen Windows-Betriebssystem aus dem Hause Microsoft. Der Kernel ist der mitunter wichtigste Bestandteil eines jeden Betriebssystems. Auf Bugtraq wurde ein Exploit veröffentlicht, mit dessen Hilfe eine Denial of Service-Schwachstelle des Network File Systems (NFSv3) ausgenutzt werden kann. NFS wird genutzt, um Dateisysteme zu exportieren; ähnlich den NetBIOS-Freigaben in der Windows-Welt. Betroffen von der Sicherheitslücke sind alle Versionen des Kernels bis und mit 2.4.20. Der Exploit führt zu einer Kernel Panic und dem Neustart des Systems. Ein Patch existiert nicht - Es wird das Update auf den neuesten Linux Kernel empfohlen. Zusätzlich sollte der Zugriff auf NFS-Ressourcen mittels Firewalling eingeschränkt werden.

Expertenmeinung:

Aufgrund der verhältnismässig hohen Verbreitung von NFS in der Unix-/Linux-Welt ist diese Schwachstelle für eine Vielzahl der Angreifer interessant. Der mit dem Bugtraq-Posting mitgelieferte Exploit stellt die Möglichkeit bereit, mal eben ein paar Maschinen abschiessen zu lassen. Besonders Skript-Kiddies werden im Laufe der nächsten Wochen Gefallen an diesem Exploit finden. Umso wichtiger ist es seine NFS-Ressourcen mittels Firewalling und aktualisiertem Kernel zu schützen.

Lösungsansatz:

Ein Upgrade auf die aktuellste Software-Version durchführen.

Bug Status:

Es ist eine aktualisierte Software-Version verfügbar.

Weiterführende Informationen finden sie auf unserer Website <http://www.scip.ch>

Adressat: Kunde
Versanddatum: 05.08.2003

scip ID: 224
Klasse: Fehlende Verschlüsselung

Securitylücke:

Novell Groupwise 5.x und 6 Clients HTTP GET Informationsleck

Vulnerability Stufe:

problematisch

Datum Publizierung:

04.08.2003

Davon betroffen:

Novell Groupwise 5.x und 6

Advisory:

<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10085583.htm>

Patch:

<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10085583.htm>

Erklärung:

Novell Groupwise 5.x und 6 Clients führen bei der Anmeldung eine HTTP GET Anfrage durch. Diese wird jeweils in den Webservern in den Log-Dateien vermerkt. Ein Angreifer mit Zugriff auf diese Daten kann Benutzernamen und die dazugehörigen Passwörter auslesen. Patching ist nicht möglich, weshalb Novell mit dem Advisory eine Anleitung zur Änderung der Konfiguration veröffentlicht hat.

Expertenmeinung:

Mit einfachsten Mitteln und ohne direktes Zutun des Angreifers ist das Ausnutzen dieser Schwachstelle möglich. Einmal zeigt ein Bug, dass ein Designfehler sehr gefährlich sein kann. In entsprechenden Umgebungen sollte man sich an die Anweisungen Novells halten, die im Advisory dokumentiert sind.

Lösungsansatz:

Die betroffene Funktion deaktivieren.

Bug Status:

Schwachstelle wurde publiziert.

Weiterführende Informationen finden sie auf unserer Website <http://www.scip.ch>

Adressat: Kunde
Versanddatum: 05.08.2003

scip ID: 226
Klasse: Denial of Service (DoS)

Securitylücke:

IPTables/Netfilter NAT Denial of Service

Vulnerability Stufe:

kritisch

Datum Publizierung:

01.08.2003

Davon betroffen:

IPTables/Netfilter mit Linux Kernel 2.4.20 und 2.5.x

Advisory:

<http://www.netfilter.org/security/2003-08-01-nat-sack.html>

Patch:

<http://www.kernel.org>

Erklärung:

IPTables/Netfilter ist eine sehr gern genutzte Möglichkeit des Firewallings unter Unix/Linux. Die meisten Distributionen liefern die entsprechenden Pakete mit. Eine Vielzahl der freien und kommerziellen Linux-Firewalls basieren gar auf diesen. Es wurden beinahe zeitgleich zwei Denial of Service-Schwachstellen in IPTables/Netfilter unter Linux Kernel 2.4.x oder 2.5.x entdeckt. Die erste ist durch die fehlerhafte Abarbeitung von NAT-Kommunikationen (Network Address Translation) gegeben. Dazu müssen die Module ip_nat_ftp, ip_nat_irc, CONFIG_IP_NF_NAT_FTP oder CONFIG_IP_NF_NAT_IRC geladen sein. Weitere Informationen zur Schwachstelle sind nicht bekannt und ein Exploit wurde auch nicht herausgegeben. Diese Schwachstelle betrifft die Versionen 2.4.20 und 2.5.x des Linux Kernels. Entsprechend wird ein Update auf einen aktualisierten Kernel empfohlen.

Expertenmeinung:

Stellt ein Linux-Rechner mit IPTables/Netfilter einen Common Point of Trust dar, was eigentlich stets der Fall sein sollte, kann sehr einfach eine flächendeckende Denial of Service-Attacke durchgeführt werden. In den meisten Umgebungen ist NAT im Einsatz, so dass dieser Angriff ein Mehr an Popularität erreichen wird.

Lösungsansatz:

Ein Upgrade auf die aktuellste Software-Version durchführen.

Bug Status:

Es ist eine aktualisierte Software-Version verfügbar.

Weiterführende Informationen finden sie auf unserer Website <http://www.scip.ch>

Adressat: Kunde
Versanddatum: 05.08.2003

scip ID: 227
Klasse: Denial of Service (DoS)

Securitylücke:

IPTables/Netfilter Connection Tracking Denial of Service

Vulnerability Stufe:

kritisch

Datum Publizierung:

02.08.2003

Davon betroffen:

IPTables/Netfilter mit Linux Kernel 2.4.20

Advisory:

<http://www.netfilter.org/security/2003-08-01-listadd.html>

Patch:

<http://www.kernel.org>

Erklärung:

IPTables/Netfilter ist eine sehr gern genutzte Möglichkeit des Firewallings unter Unix/Linux. Die meisten Distributionen liefern die entsprechenden Pakete mit. Eine Vielzahl der freien und kommerziellen Linux-Firewalls basieren gar auf diesen. Es wurden beinahe zeitgleich zwei Denial of Service-Schwachstellen in IPTables/Netfilter unter Linux Kernel 2.4.x oder 2.5.x entdeckt. Die zweite Lücke wird durch einen Fehler beim Connection Tracking von UNCONFIRMED Verbindungen realisiert. Ein Systemabsturz kann eintreten, wenn das Modul ip_conntrack geladen oder CONFIG_IP_NF_CONNTRACK aktiviert worden ist. Weitere Informationen zur Schwachstelle sind nicht bekannt und ein Exploit wurde auch nicht herausgegeben. Diese Schwachstelle betrifft nur Version 2.4.20 des Linux Kernels. Entsprechend wird ein Update auf einen aktualisierten Kernel empfohlen.

Expertenmeinung:

Stellt ein Linux-Rechner mit IPTables/Netfilter einen Common Point of Trust dar, was eigentlich stets der Fall sein sollte, kann sehr einfach eine flächendeckende Denial of Service-Attacke durchgeführt werden.

Lösungsansatz:

Ein Upgrade auf die aktuellste Software-Version durchführen.

Bug Status:

Es ist eine aktualisierte Software-Version verfügbar.

Weiterführende Informationen finden sie auf unserer Website <http://www.scip.ch>