Date and Time: 09-26-1992 at 03:21:58
Originated By: Brett Warthen (BRETT @ INFINIE)

There have been some discussions on various mailing lists over the past couple of weeks regarding security holes in NetWare. So, I thought it might be prudent to pass along some information before any rumors get out of hand.

I don't want to create any alarm or encourage attempts to break network security. I also must state up front that I personally find the actions of the Dutch Novers s mbe tremely questionable. While keeping potential security breaches secret puts the public at risk by not being able to protect themselves from the risk...making widespread announcements about such breaches to gain publicity, before giving the manufacturer a chance to address the problem is irresponsible and just creates hysteria.

While I hesitate to mention these issues any further, I know that these are the types of issues that the trade magazines tend to pick up...confuse with incomplete and inaccurate facts...and leave your boss and auditing department breathing down your neck.

The most recent security hole was exposed by a group in the Netherlands, where they demonstrated that a program running on one network work station could pretend to be another user currently signed onto the same file server. This task requires quite low level programming, and API information that is not generally published, where a program generates a network request that looks like it came from a different workstation on the network.

Novell has acknowledged this "problem", and has released a patch for NetWare 3.11 (SECURE.ZIP in NOVLIB Library 1 on CompuServe), pointing out that this problem is not just a NetWare problem, but also exists with other network operating systems.

The press releases from the Dutch Novell Users' Group and Novell are provided below FYI...

A second "security hole" is merely an old one resurfacing, one that affects versions of NetWare prior to NetWad 3re
particularly if intrudeectas turned off) there was a bug in the login validation routines, where it was possible for a program to repeatedly retry access to the file server and gain Supervisor access to the system.

This second security hole does *NOT* exist in NetWare 2.2 or 3.11, and Novell released patches for other versions of NetWare to fix this

problem. SEC286.ZIP and SEC386.ZIP are the filenames on CompuServe.

Other stories come up from time to time detailing various security threats...but it should be stressed that these other methods require physical access to the file server. Physical security of the file server is a necessity in any truly secure environment. A protected RCONSOLE password is also recommended.

========== Dutch NetWare Users' Group Press Release ================
P R E S S   R E L E A S E
September 17th, 1992

SECURITY HOLE DISCOVERED IN NOVELL NETWARE

During the LanVision event, organised by the Duch Novell User group (NGN) at Bunnik, in the Netherlands, a security problem was discovered in Novell's NetWare. With NetWare, Novell has a 70% market share of installed network operating systems.

One of the members of the NGN demonstrated the ability to obtain the authorization level of any logged in user. In this fashion, any user can aquire the same rights of any other user, e.g. the supervisor, or a financial director.

The program uses the ability to send a command to the file server such that the server "believes" that the command was issued from the other workstation. Once this is accomplished, the user is able to send commands which will function as if the privileged user had sent them.

The NGN sent the program and source code to Novell developers. The NGN urged Novell to find a solution for this problem as soon as possible, due to the severity of the problem. NGN members are developing a program that detects unauthorized usage via this particular seceakness and warns the supervisor. To the best of NGN's knowledge, the prograich ke advantage of the problem is not freely available at the present time.

The Dutch Novell User group recommendst i to melus with age of company confident ial information. Secondly, the
NGN advisesthat uers should rfrain from using the supervisor account unless noone else is working on the network.

NGN experts have reason to believe thatthe technique used, which is known as a physical attack on the wire, could be implemented on other network operating systems as well.

Editorial comments

The Dutch Novell User group (NGN) organises the LanVision event every year. It isan opprtunity to attend a 'school' for supervisors where suppliers inform supervisors about the latest news and trends concerning the networking industry. The LanVision event was an enormous success, with over 1200 supervisors attending the meeting and nearly 300 lectures being held.

The NGN, a professional user group for all network users, has the goal of improving the efficiency of the supervisor. The object of NGN is more than just a get-together of supervisors, rather the supervisor should be able to accelerate their knowledge and growth. NGN is a member of NetWare Users International (NUI), with more than 120,000 members worldwide. At more than 2000 active members, the NGN is one of the largest user groups in the world, and by far the most active user group in Europe.

You may contact the NGN office during office hours at +31 3446 1323 (CET).

========== Novell Press Release from SECURE.ZIP File ==========

MEDIA ALERT

NOVELL ENHANCES NETWARE SECURITY

Novell today announced that it has enhanced NetWare security by developing and making available software enhancements for its NetWare v3.x, NetWare v2.x and NetWare for Unix customers. These enhancements are designed to counteract a recently discovered security threat to network operating systems.

The security threat, proven in a Netherlands academic laboratory, is not currently found in commercial environments and requires the hacker to forge requests on the wire in the name of a more privileged user. However, Novell considers any threat, even a potential threat, to network security to be serious and has worked quickly to develop and provide solutions for its customers.

Because this security threat affects other network operating systems, it is an industry-wide problem. In addition to being the first to address this security threat for its customers, Novell is willing to work closely with other companies in the industry to ensure that in general networks are as secure as possible.

Novell is also continuing its education efforts to ensure that customers have the most secure network environments available. Novell recommends that all customers who are concerned about security activate all applicable NetWare security features and install the most recent versions of system software, client software and patches.

Novell will make the software enhancements available on NetWire and NetWare

Express for NetWare v3.x and NetWare v2.x customers. The enhancements will also be given directly to NetWare for Unix partners so that they can make the solution available to their customers.

========== Novell Technical Bulletin from SECURE.ZIP ==========

NOVELL TECHNICAL BULLETIN

TITLE: Physical Security of a NetWare Server
DOCUMENT ID#: TB.P.287
DATE: 12APR91
PRODUCT: NetWare
PRODUCT VERSION:
SUPERSEDES: NA

SYMPTOM: NA

ISSUE/PROBLEM

It is necessary to reiterate the need to physically secure a NetWare server. Some NetWare administrators may not be aware of this security measure. Precautions, such as those implemented in the mainframe and minicomputer environment, should also be taken to physically protect the server from unauthorized use in a NetWare environment. If the server is not secured in a locked area, unauthorized users may be able to down the server and remove devices; destroy data and system configuration; and otherwise gain access to sensitive information.

In addition to securing the server, NetWare provides a number of security features that help protect the server console and system from misuse. The following are functions that can be used to enhance server security on a NetWare operating system.

~ Issue the SECURE CONSOLE command from a NetWare v3.x console. By doing this, the system will only load NLMs from SYS:SYSTEM.

~ Select Lock File Server Console from the NetWare v3.x MONITOR.NLM main menu. This will password-protect the server console.

~ Protect RCONSOLE.NLM from a NetWare v3.x system with a password.

~ Use other security features of NetWare v2.x and v3.x such as intruder detection, forced password changes, limited grace logins, etc.

~ Use server hardware password protetion if available.

These advanced features enhance system security, but do not remove the need to place the server in a secure location. NetWare security features

combined with physical protection of the server affords the system administrator the highest server security possible in the NetWare environment.

========== End Novell Technical Bulletin ==========

Brett Warthen	MHS: Brett @ Infinite (via NHUB/CSERVE)
Infinite Technologies	CompuServe: >MHS:Brett@Infinite
11433 Cronridge Drive	Internet: Brett@Infinite.mhs.compuserve.com
Suite H	FAX: +1-410-363-3779
Owings Mills, MD 21117	Fone: +1-410-363-1097

Damn, sure didn't import to well on the upload, but I think it is still readable. Anyone have any friends in the Netherlands? Wouldn't mind having a copy of that program or at least know what API calls they use that aren't documented.