Software Engineering Institute
Carnegie Mellon University

1998 CERT Incident Notes

CERT Division

http://www.sei.cmu.edu

REV-03.18.2016.0

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 IN-98.01: Scans to Port 1/tcpmux and unpassworded SGI accounts

Wednesday, May 13, 1998

For the past couple of weeks we have received reports of widespread scans to TCP port 1. The service assigned to TCP port 1 is tcpmux (for more info see RFC#1078). We know that some of the scans originated from sites which were root compromised.

We were able to obtain files from a site which was used to launch these scans which indicate that the intruder was scanning for IRIX machines. By default, IRIX systems have tcpmux enabled. Once the intruder had found a number of machines with a service running on port 1/tcpmux, another automated intruder tool was used to telnet to each of these machines and attempt to log in as guest, lp, and demos.

In addition to the above incident, we have noticed an increase in the number of reports of IRIX root compromises over the past few weeks. We have also received numerous independent reports of widespread failed login attempts to lp, guest, demos, OutOfBox, and EZsetup accounts.

We have been in communication with SGI about this issue. At this time there does not appear to be any vulnerability in the SGI implementation of tcpmux or any service provided through tcpmux.

IRIX machines ship by default with unpassworded accounts. As of IRIX 6.3 there is a security tool to easily disable or add passwords to these accounts at installation time. Please refer to the following advisories for more information about this issue:

- ftp://sgigate.sgi.com/security/19951002-01-I
- http://www.cert.org/advisories/CA-95.15.SGI.lp.vul.html

We strongly encourage you to ensure that the full set of security patches for each of your systems is applied. This is a major step in defending your systems from attack, and its importance cannot be overstated.

We encourage you to check with your vendor regularly for any updates or new patches that relate to your systems. We also encourage you to ensure that you are up to date with patches and workarounds referenced in CERT advisories.

IRIX patches are available from:

- http://www.sgi.com/support/security/index.html

If your IRIX machine has unpassworded accounts, then aside from disabling (or adding password protection to) accounts which do not have passwords, we encourage you to inspect your system for signs of intrusion. For instructions on how to do this please refer to the "Recovering from an Incident" web page.

This document is available from: http://www.cert.org/incident_notes/IN-98.01.irix.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

2 IN-98.02: New Tools Used For Widespread Scans

Thursday, July 2, 1998

Intruders launching widespread scans in order to locate vulnerable machines is nothing new; however, a new intruder tool was publicly released last week which scans networks for many different vulnerabilities. The CERT Coordination Center has received numerous reports indicating that this tool is in widespread use within the intruder community.

The tool uses both DNS zone transfers and/or brute force scanning of IP addresses to locate machines. Once machines are located, they are tested for a number of vulnerabilities.

The tool has the capability to test for the following vulnerabilities:

- statd vulnerability - see http://www.cert.org/advisories/CA-97.26.statd.html
- imap/pop3 vulnerabilities - see http://www.cert.org/advisories/CA-97.09.imap_pop.html
- IRIX machines that have accounts with no passwords - see http://www.cert.org/advisories/CA-95.15.SGI.lp.vul.html
- bind vulnerability - see http://www.cert.org/advisories/CA-98.05.bind_problems.html
- cgi-bin vulnerabilities - see http://www.cert.org/tech_tips/cgi_metacharacters.html
    - phf - see http://www.cert.org/advisories/CA-96.06.cgi_example_code.html
    - handler - see ftp://ftp.cert.org/pub/cert_bulletins/VB-97.07.sgi
    - test-cgi
- NFS filesystems exported to everyone
- X11 (open X servers)

We encourage you to ensure that all machines in your network utilizing any of the above services are up to date with patches and properly secured.

The footprints of this attack are sequential connections to multiple hosts on one or more of the following TCP ports.

```
Port   Service
--------------
(23)   telnet
(53)   dns
(79)   finger
(80)   web
(110)  pop
(111)  SunRPC & NFS (UDP and TCP)
(143)  imap
(1080) socks
(2049) nfs (UDP)
(6000) X
```

Also, requests for the phf, handler, and test-cgi CGI scripts may show up in web access logs.

We encourage sites to disable or add access control to DNS zone transfers. One way to do this is to filter port 53 (TCP) to prevent domain name service zone transfers and permit access to socket 53 (TCP) only from known secondary domain name servers.

We also urge you to filter/firewall all traffic except that which you explicitly decide to allow. Please look at our packet filtering tech tip for more information: http://www.cert.org/tech_tips/packet_filtering.html

This document is available from: http://www.cert.org/incident_notes/IN-98.02.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

3 IN-98.03: Password Cracking Activity

DATE: Thursday, July 16, 1998

In an incident recently reported to the CERT/CC, a very large collection of password files was found on a compromised system.

In total, the intruder appears to have a list of 186,126 accounts and encrypted passwords. At the time the password file collection was discovered, the intruder had successfully guessed 47,642 of these passwords by using a password-cracking tool.

Since most of the entries did not come from the site where the collection was found, it appears that they were collected from other sites by the intruder. While some of the password files included information identifying the site where the file originated, over 160,000 of the entries include only a userid and an encrypted password.

If your site could have been identified as involved in this incident, the system administrator of the compromised host would have already contacted you regarding this activity.

The collection is reported to contain entries from at least one password file that was originally shadowed. The intruder is also reported to have a collection of passwords that appear to have been obtained using network sniffing software. This list of passwords is apparently being used as input to the password-cracking tool.

If you are interested in more information about protecting your systems against password-cracking attacks, you may want to review our Tech Tip on this topic: http://www.cert.org/tech_tips/passwd_file_protection.html.

This document is available from: http://www.cert.org/incident_notes/IN-98.03.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

4 IN-98.04: Advanced Scanning

Tuesday, September 29, 1998

We have received reports of two scanning techniques being used by intruders to map networks and identify systems:

- "Stealth" scanning
- Scanning to identify system or network architecture

In addition to the reports we have received, the Dahlgren Division of the Naval Surface Warfare Center has published information indicating that multiple intruders may be using these attacks in a coordinated effort. This information is available at http://www.nswc.navy.mil/ISSEC/CID/co-ordinated_analysis.txt.

Stealth Scanning

The "stealth" scans appear to have a common goal: to gather information about target sites while avoiding detection by using techniques that might be overlooked by intrusion detection systems and system administrators. These techniques include

- **Inverse Mapping**
  In an 'Inverse Mapping' scan, intruders send packets that normally would go unnoticed or cause no unusual behavior to a list of addresses. For hosts that do not exist, however, routers will return an ICMP host unreachable message. By determining what hosts do not exist, an intruder can infer what hosts do exist, and so gain information about the structure of your network.

  Any packet type can be used to generate the ICMP host unreachable message, but we have received reports that intruders are actively using RESET packets, SYN-ACK packets, and DNS response packets for which no query was ever made.

- **Slow Scans**
  In a "slow scan" intruders scan the network at a slow rate that is likely to avoid detection. These types of scans are difficult to detect automatically, because you must maintain a history of all the packets you've received in order to detect new packets that may be related to old traffic.

Scanning to Identify System or Network Architecture

Intruders have also employed scanning techniques to identify the operating system used by a particular host, or to determine information about the structure of the target network. A tool recently released, called *queso*, relies on the variations in response to unexpected packets to determine the operating system of a particular host.

That is, *queso* sends unexpected packets to a host and examines the response. Because the packets are unexpected, there is no standard response, and so each operating system is free to respond in a unique way. By examining the responses to these unexpected packets, *queso* can determine the kinds of operating systems and TCP/IP stacks installed on your network. This information can be used by an intruder to optimize attacks on your network, or to identify sets of machines with particular vulnerabilities.

This is similar in effect to the scans described in http://www.cert.org/incident_notes/IN-98.01.irix.html except that queso recognizes a variety of operating systems, whereas the scans described in Incident Note 98.01 recognized only IRIX.

The following excerpt from tcpdump shows a queso probe against a machine running Solaris 2.5.1. (Information in boldface type indicates the target system's first response packet.)

```
server.24728 > solaris1.local.10.in-addr.arpa.telnet: S
1119794168:1119794168(0) win 4660
solaris1.local.10.in-addr.arpa.telnet > server.24728: S
442322772:442322772(0) ack 1119794169 win 9112 <mss 536> (DF)
server.24728 > solaris1.local.10.in-addr.arpa.telnet: R
1119794169:1119794169(0) win 0
server.24729 > solaris1.local.10.in-addr.arpa.telnet: S
1119794168:1119794168(0) ack 0 win 4660
solaris1.local.10.in-addr.arpa.telnet > server.24729: R 0:0(0) win 0
(DF)
server.24730 > solaris1.local.10.in-addr.arpa.telnet: F
1119794168:1119794168(0) win 4660
server.24731 > solaris1.local.10.in-addr.arpa.telnet: F
1119794168:1119794168(0) ack 0 win 4660
solaris1.local.10.in-addr.arpa.telnet > server.24731: R 0:0(0) win 0
(DF)
server.24732 > solaris1.local.10.in-addr.arpa.telnet: SF
1119794168:1119794168(0) win 4660
solaris1.local.10.in-addr.arpa.telnet > server.24732: S
442455494:442455494(0) ack 1119794169 win 9112 <mss 536> (DF)
server.24732 > solaris1.local.10.in-addr.arpa.telnet: R
1119794169:1119794169(0) win 0
server.24733 > solaris1.local.10.in-addr.arpa.telnet: P win 4660
server.24734 > solaris1.local.10.in-addr.arpa.telnet: S
1119794168:1119794168(0) win 4660
solaris1.local.10.in-addr.arpa.telnet > server.24734: S
442581319:442581319(0) ack 1119794169 win 9112 <mss 536> (DF)
server.24734 > solaris1.local.10.in-addr.arpa.telnet: R
1119794169:1119794169(0) win 0
```

The following excerpt, also from tcpdump, shows a *queso* probe against a machine running NT Workstation 4.0:

```
server.5856 > ntwork1.nt.local.netbios-ssn: S
1276897729:1276897729(0) win 4660
ntwork1.nt.local.netbios-ssn > server.5856: S 285465669:285465669(0)
ack 1276897730 win 8576 <mss 1460> (DF)
server.5856 > ntwork1.nt.local.netbios-ssn: R
1276897730:1276897730(0) win 0
server.5857 > ntwork1.nt.local.netbios-ssn: S
1276897729:1276897729(0) ack 0 win 4660
ntwork1.nt.local.netbios-ssn > server.5857: R 0:0(0) win 0
server.5858 > ntwork1.nt.local.netbios-ssn: F
1276897729:1276897729(0) win 4660
ntwork1.nt.local.netbios-ssn > server.5858: R 0:0(0) ack 1276897730
win 0
server.5859 > ntwork1.nt.local.netbios-ssn: F
1276897729:1276897729(0) ack 0 win 4660
ntwork1.nt.local.netbios-ssn > server.5859: R 0:0(0) win 0
server.5860 > ntwork1.nt.local.netbios-ssn: SF
1276897729:1276897729(0) win 4660
ntwork1.nt.local.netbios-ssn > server.5860: S 285465749:285465749(0)
ack 1276897730 win 8576 <mss 1460> (DF)
server.5860 > ntwork1.nt.local.netbios-ssn: R
1276897730:1276897730(0) win 0
server.5861 > ntwork1.nt.local.netbios-ssn: P win 4660
ntwork1.nt.local.netbios-ssn > server.5861: R 0:0(0) ack 1276897729
win 0
server.5862 > ntwork1.nt.local.netbios-ssn: S
1276897729:1276897729(0) win 4660
ntwork1.nt.local.netbios-ssn > server.5862: S 285465789:285465789(0)
ack 1276897730 win 8576 <mss 1460> (DF)
server.5862 > ntwork1.nt.local.netbios-ssn: R
1276897730:1276897730(0) win 0
```

Note that the responses of the two operating systems differ as early as the first response packet (highlighted above). By comparing these differences to a dictionary of known response characteristics, *queso* is often able to determine the type of operating system employed by the target machine. Users can also extend *queso* to distinguish other kinds of operating systems, or other devices that will respond to TCP/IP packets.

We have received reports of incidents in which intruders have launched coordinated scans that may have been used to discover information about the structure of the target network. By launching similar scans from two or more distinct networks against a single target network, and then comparing the different responses, intruders may be able to infer information about the structure of the target network. By using two or more networks to launch a scan against a third network, an intruder can

- Discover alternate routes into your network
- Infer aspects of the topology of your network
- Increase the bandwidth available to launch a denial of service attack
- Reduce the likelihood of detection

Conclusion

Intruders are using a variety of techniques to gain information about networks and systems on those networks. Intruders can use this information to tailor their attacks to target networks or to find a set of machines that share a certain vulnerability.

Intruders have recently used a number of very large-scale scans of the Internet looking for certain vulnerabilities, such as those discussed in http://www.cert.org/incident_notes/IN-98.02.html

The ability to determine the types of operating systems in use helps intruders to focus their attacks on certain types of machines, or to modify their attacks to suit the target.

Do not presume that the topology of your network, the operating systems in use, the products used to connect to the Internet, and other externally visible characteristics are a secret. When you evaluate the security of your network, remember that this information can be discovered by intruders who can use it to their advantage.

Acknowledgements

Our thanks to Stephen Northcutt of the Naval Surface Warfare Center for his assistance.

This document is available from: http://www.cert.org/incident_notes/IN-98.04.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

5 IN-98-05: Probes with Spoofed IP Addresses

Wednesday, November 24, 1998

The CERT Coordination Center has received several reports that intruders are using spoofed IP addresses to conduct scans similar to those discussed in
http://www.cert.org/advisories/CA-98.09.imapd.html
http://www.cert.org/advisories/CA-97.09.imap_pop.html

At first, these probes appeared to be ordinary IMAP scans. After further investigation, most of these sites determined that another compromised host on the same network was the true origin of the IMAP scan. It's possible that the intruder was able to run a network sniffer to capture the results of these probes.

If IMAP (or other) probes are reported to originate from hosts at your site, it may not be sufficient to disconnect the apparent origin from the network. We encourage you to inspect other hosts on the same local area network, especially if you continue to receive reports of intruder activity involving your systems.

You may find our Intruder Detection Checklist to be a useful guide in checking your systems for signs of compromise. This document is available from our ftp server at
http://www.cert.org/tech_tips/intruder_detection_checklist.html

This document will help you to methodically check your systems for signs of compromise and offers pointers to other resources and suggestions on how to proceed in the event of a compromise.

Another approach to determine the true origin of spoofed probes is to install network monitoring software which can capture the packets actually traversing the network. Some network monitoring software logs may include the hardware (ethernet) address of the true origin of the probes. This information may enable you to determine which system is generating the spoofed probes by comparing the hardware address with those of other systems on the local area network.

While probes fitting this profile have thus far originated only from port 65535, it's possible that spoofed probes could come from other ports.

If you believe that your systems have been compromised and used to launch probes fitting this description, we encourage you to report the activity to the CERT/CC. In particular, we are interested in receiving copies of any intruder tools that have been used to generate spoofed probes or to capture the results.

This document is available from: http://www.cert.org/incident_notes/IN-98-05.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

6 IN-98-06: Automated Scanning and Exploitation

Wednesday, December 9, 1998

The CERT Coordination Center has received reports of intruders executing widespread attacks using scripted tools to control a collection of information-gathering and exploitation tools. The combination of functionality used by the scripted tools enables intruders to automate the process of identifying and exploiting known vulnerabilities in specific host platforms.

One scripted tool we are aware of uses a port scanning tool to perform widespread scanning to identify hosts responding on TCP port 111 (portmapper). This functionality is similar to the widespread scanning activity discussed in CERT Incident Note IN-98.02:

http://www.cert.org/incident_notes/IN-98.02.html

The scripted tool then uses an advanced scanning tool to attempt to identify the operating system architecture of hosts identified in the widespread scanning. The scripted tool looks for hosts identified to be running Linux. This functionality is similar to the advanced scanning techniques described in CERT Incident Note IN-98.04:

http://www.cert.org/incident_notes/IN-98.04.html

For each host identified as responding on TCP port 111 and appearing to be running Linux, the scripted tool uses an exploit tool to attempt exploitation of the mountd vulnerability described in CERT Advisory CA-98.12:

http://www.cert.org/advisories/CA-98.12.mountd.html

If the exploit tool is successful in gaining privileged access to the host, the exploit tool executes a series of shell commands to provide the intruder with a passwordless privileged account.

The scripted tool then logs the hostname of each compromised host to a file.

Conclusion

To help protect your systems from the various automated tools being used by the intruder community, we urge you to ensure that all machines in your network are up to date with patches and properly secured.

This document is available from: http://www.cert.org/incident_notes/IN-98-06.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

7 IN-98-07: Windows NT "Remote Explorer" Virus

December 22, 1998

Recently, a Windows NT virus by the name of "Remote Explorer" or "RICHS" has received some public attention. Although this virus can modify files, our interaction with Microsoft leads us to belive that this virus is unable to gain any privileges beyond those of the user running the infected program. That is, the virus has only the capabilities, file permissions, etc.,of the person running it.

However, in addition to being an ordinary virus, Remote Explorer can also install itself as a Windows NT service if an infected file is run by someone with local administrator privileges. Once it has been installed as a service, Remote Explorer can impersonate anyone else who subsequently logs into the system, including domain administrators. Then, using the privileges of a domain administrator, Remote Explorer attempts to self-propagate by infecting other files on the network. Note that the ability to impersonate the currently-logged-in user is an ordinary function of any service that has been installed with privileges.

The additional ability to install itself as a service probably means that Remote Explorer can propogate somewhat faster than other viruses.

The CERT Coordination Center has not received any first-hand reports of this virus infecting systems or networks, though we have received one second-hand report of the infection of approximately 50 Windows NT servers and an undetermined number of Windows NT workstations.

You can identify machines infected by current strains of the virus by looking for a service running as "Remote Explorer" in the services control panel.

In general, we recommend that sites adhere to the following practices:

- Log in with administrative privileges only when needed. Avoid doing ordinary tasks with enhanced privileges.
- Log in as a Domain Administrator only from trusted workstations.
- Install and maintain anti-virus tools.
- Avoid running executables from unknown or untrusted sources.
- Educate users about anti-virus policies

Microsoft has provided some information regarding Remote Explorer. For more information, please see http://www.microsoft.com/security/bulletins/remote.asp.

Contributors

Our thanks to Jason Garms of Microsoft for reporting this problem to us and providing technical assistance.

This document is available from: http://www.cert.org/incident_notes/IN-98-07.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site:
http://www.cert.org/

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.
