CERT Advisory CA-1995-18 Widespread Attacks on Internet Sites

Original issue date: December 18, 1995
Last revised: September 23, 1997
Updated copyright statement

A complete revision history is at the end of this file.

Over the last several weeks, the CERT Coordination Center has been working on a set of incidents in which the intruders have launched widespread attacks against Internet sites. Hundreds of sites have been attacked, and many of the attacks have been successful, resulting in root compromises at the targeted sites. We continue to receive reports, and we believe that more attacks are going undetected.

All the vulnerabilities exploited in these attacks are known, and are addressed by CERT advisories (see Section III).

We urge everyone to obtain these advisories and take action to ensure that systems are protected against these attacks. Also, please feel free to redistribute this message.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

Also see CERT Summaries for information on intruder activity:
ftp://ftp.cert.org/pub/cert_summaries/

I. Description

Intruders are doing the following:

- using automated tools to scan sites for NFS and NIS vulnerabilities
- exploiting the rpc.ypupdated vulnerability to gain root access

- exploiting the loadmodule vulnerability to gain root access

- installing Trojan horse programs and packet sniffers

- launching IP spoofing attacks

II. Impact

Successful exploitation of the vulnerabilities can result in unauthorized root access.

III. Solution

The CERT staff urges you to immediately take the steps described in the advisories listed below. Note that it is important to check advisories periodically as we add updated information as we receive it.

a. Using automated tools to scan sites for NFS and NIS vulnerabilities

- CA-94.15.NFS.Vulnerabilities
- CA-92.13.SunOS.NIS.vulnerability

b. Exploiting the rpc.ypupdated vulnerability to gain root access

- CA-95.17.rpc.ypupdated.vul

c. Exploiting the loadmodule vulnerability to gain root access

- CA-93.18.SunOS.Solbourne.loadmodule.modload.vulnerability
- A-95.12.sun.loadmodule.vul

d. Installing Trojan horse programs and packet sniffers

- CA-94.01.ongoing.network.monitoring.attacks

e. Launching IP spoofing attacks

- CA-95.01.IP.spoofing

The CERT advisories are available from

ftp://ftp.cert.org/pub/cert_advisories

If you find a compromise, please complete the Incident Reporting Form that we have provided at the end of this advisory, and return the form to cert@cert.org. This completed form will help us better assist you.

Note: Because of our workload, we must ask you not to send log files of activity, but we would be happy to work with you as needed on how to interpret data that you may collect. Also, the CERT staff can provide guidance and advice, if needed, on how to handle incidents and work with law enforcement.

Appendix: Incident Reporting Form

(also available from ftp://ftp.cert.org/pub/incident_reporting_form)

version 3.0

CERT* Coordination Center
Incident Reporting Form

The CERT Coordination Center (CERT/CC) has developed the following form in an effort to gather incident information. We would appreciate your completing the form below in as much detail as possible. The information is optional, but from our experience we have found that having the answers to all the questions enables us to provide the best assistance. Completing the form also helps avoid delays while we get back to you requesting the information we need in order to help you. Sites have told us, as well, that filling out the form has helped them work through the incident.

Note that our policy is to keep any information specific to your site confidential unless we receive your permission to release that information.

Please feel free to duplicate any section as required. Please return this form to cert@cert.org. If you are unable to email this form, please send it by FAX. The CERT/CC FAX number is

+1 412 268 6989

Thank you for your cooperation and help.

```
1.0. General Information

     1.1. Incident number (to be assigned by the CERT/CC):  CERT#

     1.2. Reporting site information

          1.2.1.  Name (e.g., CERT Coordination Center):
          1.2.2.  Domain Name (e.g., cert.org):
          1.2.3.  Brief description of the organization:
          1.2.4.  Is your site an Internet Service Provider (Yes/No):


2.0. Contact Information

     2.1. Your contact information

           2.1.1.  Name:
           2.1.2.  Email address:
           2.1.3.  Telephone number:
           2.1.4.  FAX number:
           2.1.5.  Pager number:
           2.1.6.  Home telephone number (for CERT/CC internal use only):
           2.1.7.  Secure communication channel (e.g., PGP, PEM, DES, secure
                    telephone/FAX) [NOTE -- we will call to obtain the secure
                    communication channel information] (Yes/No):

     2.2. Additional contact information (if available)

           2.2.1.  Name:
           2.2.2.  Email address:
           2.2.3.  Telephone number:
           2.2.4.  FAX number:
           2.2.5.  Pager number:
           2.2.6.  Home telephone number (for CERT/CC internal use only):
           2.2.7.  Secure communication channel (Yes/No):

     2.3. Site security contact information (if applicable)

           2.3.1.  Name:
           2.3.2.  Email address:
           2.3.3.  Telephone number:
           2.3.4.  FAX number:
           2.3.5.  Pager number:
           2.3.6.  Home telephone number (for our internal use only):
           2.3.7.  Secure communication channel (Yes/No):

     2.4. Contact information for other site(s) involved in this incident (if
```

available)

2.4.1. Site name:
2.4.2. Contact person name:
2.4.3. Email address:
2.4.4. Telephone number:
2.4.5. FAX number:
2.4.6. Pager number:
2.4.7. Home telephone number (for CERT/CC internal use only):
2.4.8. Secure communication channel (Yes/No):

2.5. Contact information for any other incident response team(s) (IRTs) that has/have been notified (if available)

2.5.1. IRT name:
2.5.2. Constituency domain:
2.5.3. Contact person name:
2.5.4. Email address:
2.5.5. Telephone number:
2.5.6. FAX number:
2.5.7. Pager number:
2.5.8. Home telephone number (for CERT/CC internal use only):
2.5.9. Secure communication channel (Yes/No):
2.5.10. IRT reference number:

2.6. Contact information for any law enforcement agency(ies) that has/have been notified (if available)

2.6.1. Law enforcement agency name:
2.6.2. Contact person name:
2.6.3. Email address:
2.6.4. Telephone number:
2.6.5. FAX number:
2.6.6. Pager number:
2.6.7. Home telephone number (for CERT/CC internal use only):
2.6.8. Secure communication channel (Yes/No):
2.6.9. Law enforcement agency reference number:

3.0. Contacting Sites Involved

3.1. We ask that reporting sites contact other sites involved in incident activity. Please let us know if you need assistance in obtaining contact information for the site(s) involved.

When contacting the other sites, we would very much appreciate a cc to the "cert@cert.org" alias. This helps us identify connections between incidents and understand the scope of intruder activity. We would also appreciate your including our incident number in the subject line of any correspondence relating to this incident if one has been assigned (see item 1.1.).

If you are unable to contact the involved sites, please get in touch with us to discuss how we can assist you.

3.2. Disclosure information -- may we give the following types of information to

3.2.1. the sites involved in this incident

3.2.1.1. your domain (Yes/No):
3.2.1.2. your host(s) involved (Yes/No):
3.2.1.3. your contact information (Yes/No):

3.2.2. incident response teams, for sites from their constituencies involved in this incident

3.2.2.1. your domain (Yes/No):
3.2.2.2. your host(s) involved (Yes/No):
3.2.2.3. your contact information (Yes/No):

3.2.3. law enforcement agency(ies) if there is a legal investigation

3.2.3.1. your domain (Yes/No):
3.2.3.2. your host(s) involved (Yes/No):
3.2.3.3. your contact information (Yes/No):

4.0. Host Information

4.1. Host(s) involved at your site. Please provide information on all host(s) involved in this incident at the time of the incident (one

entry per host please)

4.1.1. Hostname:
4.1.2. IP address(es):
4.1.3. Vendor hardware, OS, and version:
4.1.4. Security patches applied/installed as currently recommended by the vendor and the CERT/CC (Yes/No/Unknown):
4.1.5. Function(s) of the involved host

4.1.5.1. Router (Yes/No):
4.1.5.2. Terminal server (Yes/No):
4.1.5.3. Other (e.g. mail hub, information server, DNS [external or internal], etc.):

4.1.6. Where on the network is the involved host (e.g. backbone, subnet):
4.1.7. Nature of the information at risk on the involved host (e.g., router configuration, proprietary, personnel, financial, etc.):
4.1.8. Timezone of the involved host (relative to GMT):
4.1.9. In the attack, was the host the source, the victim, or both:
4.1.10. Was this host compromised as a result of this attack (Yes/No):

4.2. Host(s) involved at other other sites (one entry per host please)

4.2.1. Hostname:
4.2.2. IP address(es):
4.2.3. Vendor hardware, OS, and version:
4.2.4. Has the site been notified (Yes/No):
4.2.5. In the attack, was the host the source, the victim, or both:
4.2.6. Was this host compromised as a result of this attack (Yes/No):

5.0. Incident Categories

5.1. Please mark as many categories as are appropriate to this incident

5.1.1. Probe(s):
5.1.2. Scan(s):
5.1.3. Prank:
5.1.4. Scam:
5.1.5. Email Spoofing:
5.1.6. Email bombardment:

5.1.6.1. was this denial-of-service attack successful (Yes/No):

5.1.7. Sendmail attack:

5.1.7.1. did this attack result in a compromise (Yes/No):

5.1.8. Break-in

5.1.8.1. Intruder gained root access (Yes/No):
5.1.8.2. Intruder installed Trojan horse program(s) (Yes/No):
5.1.8.3. Intruder installed packet sniffer (Yes/No):

5.1.8.3.1. What was the full pathname(s) of the sniffer output file(s):
5.1.8.3.2. How many sessions did the sniffer log? (use "grep -c 'DATA' <filename>" to obtain this information):

5.1.8.4. NIS (yellow pages) attack (Yes/No):
5.1.8.5. NFS attack (Yes/No):
5.1.8.6. TFTP attack (Yes/No):
5.1.8.7. FTP attack (Yes/No):
5.1.8.8. Telnet attack (Yes/No):
5.1.8.9. Rlogin or rsh attack (Yes/No):
5.1.8.10. Cracked password (Yes/No):
5.1.8.11. Easily-guessable password (Yes/No):

5.1.9. Anonymous FTP abuse (Yes/No):
5.1.10. IP spoofing (Yes/No):
5.1.11. Product vulnerability (Yes/No):

5.1.11.1. Vulnerability exploited:

5.1.12. Configuration error (Yes/No):

5.1.12.1. Type of configuration error:

5.1.13. Misuse of host(s) resources (Yes/No):
5.1.14. Worm (Yes/No):
5.1.15. Virus (Yes/No):
5.1.16. Other (please specify):

6.0. Security Tools

6.1. At the time of the incident, were you any using the following security tools (Yes/No; How often)

Network Monitoring tools
6.1.1. Argus:
6.1.2. netlog (part of the TAMU Security Package):

Authentication/Password tools
6.1.3. Crack:
6.1.4. One-time passwords:
6.1.5. Proactive password checkers:
6.1.6. Shadow passwords:
6.1.7. Kerberos:

Service filtering tools
6.1.8. Host access control via modified daemons or wrappers:
6.1.9. Drawbridge (part of the TAMU Security Package):
6.1.10. Firewall (what product):
6.1.11. TCP access control using packet filtering:

Tools to scan hosts for known vulnerabilities
6.1.12. ISS:
6.1.13. SATAN:

Multi-purpose tools
6.1.14. C2 security:
6.1.15. COPS:
6.1.16. Tiger (part of the TAMU Security Package):

File Integrity Checking tools
6.1.17. MD5:
6.1.18. Tripwire:

Other tools
6.1.19. lsof:
6.1.20. cpm:
6.1.21. smrsh:
6.1.22. append-only file systems:

Additional tools (please specify):

6.2. At the time of the incident, which of the following logs were you using, if any (Yes/No)

6.2.1. syslog:
6.2.2. utmp:
6.2.3. wtmp:
6.2.4. TCP wrapper:
6.2.5. process accounting:

6.3. What do you believe to be the reliability and integrity of these logs (e.g., are the logs stored offline or on a different host):

7.0. Detailed description of the incident

7.1. Please complete in as much detail as possible

7.1.1. Date and duration of incident:
7.1.2. How you discovered the incident:
7.1.3. Method used to gain access to the affected host(s):
7.1.4. Details of vulnerabilities exploited that are not addressed in previous sections:
7.1.5. Other aspects of the "attack":
7.1.6. Hidden files/directories:
7.1.7. The source of the attack (if known):
7.1.8. Steps taken to address the incident (e.g., binaries reinstalled, patches applied):
7.1.9. Planned steps to address the incident (if any):

```
          7.1.10. Do you plan to start using any of the tools listed
                  above in question 6.0 (please list tools expected
                  to use):
          7.1.11. Other:

     7.2. Please append any log information or directory listings and
          timezone information (relative to GMT).

     7.3. Please indicate if any of the following were left on your
          system by the intruder (Yes/No):

          7.3.1. intruder tool output (such as packet sniffer output
                 logs):
          7.3.2. tools/scripts to exploit vulnerabilities:
          7.3.3. source code programs (such as Trojan horse programs,
                 sniffer programs):
          7.3.4. binary code programs (such as Trojan horse programs,
                 sniffer programs):
          7.3.5. other files:

          If you answered yes to any of the last 5 questions, please call
          the CERT/CC hotline (+1 412 268 7090) for instructions on
          uploading files to us by FTP.  Thanks.

     7.4. What assistance would you like from the CERT/CC?
```

Revision History

```
Sep. 23, 1997  Updated copyright statement
Aug. 30, 1996 - Removed references to README files because updated information
                  is put into the advisories themselves.
                Added a pointer to CERT summaries.
                Updated the file name for the incident reporting form (IRF).
                Replaced the old version of the IRF with version 3.0.
```