CERT Advisory CA-1995-07 SATAN Vulnerability: Password Disclosure

Original issue date: April 21, 1995
Last revised: September 23, 1997
Update copyright statement

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

This is a revised CERT advisory.
It addresses inaccurate information in CA-95.07
and contains information about SATAN 1.1.1.
Supersedes CA-95.07

There was a potential vulnerability introduced into systems running SATAN 1.0 and earlier, as described below. The problem has been addressed in version 1.1 and later. The CERT/CC team recommends that you take the precautions described in Section III below before you run SATAN and that you upgrade to the latest version of SATAN--currently 1.1.1.

The following two statements from CA-95.07 are inaccurate.

1. This statement is incorrect: "Note that SATAN 1.1 is expected to check systems for this SATAN 1.0 vulnerability as part of scanning other systems."
2. This statement is misleading: "This vulnerability affects all systems that support the use of SATAN with the HTML interface." For SATAN 1.0 and earlier, whether a system is vulnerable depends on the system configuration, the net browser supporting SATAN, and how SATAN is used. The problem has been solved in later versions of SATAN.

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

For an overview of a beta version of SATAN, see CERT advisory CA-95.06.

I. Description

In SATAN version 1.0, access to the SATAN processes is protected by a session key (also referred to as a "magic cookie" or "password"). SATAN itself never sends this session key over the network. However, depending on the configuration at your site, the supporting HTML browser, and how you use SATAN, your session key may be disclosed through the network. Local or remote users who obtain your session key can run perl scripts that are on the system running SATAN.

If you use SATAN only through the command line interface, your system is not vulnerable to the problem because there is no session key.

Additional details are in the "SATAN Password Disclosure" tutorial provided with SATAN. We have included the tutorial as an Appendix B of this advisory.

II. Impact

If the session key is disclosed while SATAN 1.0 is running, unauthorized local or remote users can execute perl scripts as the user of the process running SATAN (typically root).

III. Solution

1. Obtain and install SATAN version 1.1.1, which addresses the problem.

For details on how the problem is addressed, see the section entitled "Additional SATAN Defenses" in the SATAN Password Disclosure tutorial. The SATAN authors also provide guidance on protecting access; see the tutorial section, "Preventing SATAN Password Disclosure." SATAN 1.1.1 is available from many sites, including

ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.tar.Z
ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.README
ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.tar.Z.asc

MD5 (satan-1.1.1.tar.Z) = de2d3d38196ba6638b5d7f37ca8c54d7
MD5 (satan-1.1.1.README) = 3f935e595ab85ee28b327237f1d55287
MD5 (satan-1.1.1.tar.Z.asc) = a9261070885560ec11e6cc1fe0622243

To locate other sites, you can send mail to

majordomo@wzv.win.tue.nl

and put in the body of the message (not the subject line):

get satan mirror-sites

There are reports of modified copies of SATAN, so ensure that the copy that you obtain is authentic by checking the MD5 checksum or SATAN author Wietse Venema's PGP signature. Appendix A of this advisory contains his PGP key.

We urge you to read the SATAN documentation carefully before running SATAN.

2. We also recommend that you take the following precautions:

- Install all relevant security patches for the system on which you will run SATAN.
- Execute SATAN only from the console of the system on which it is installed (e.g., do not run SATAN from an X terminal, from a diskless workstation, or from a remote host).
- Ensure that the SATAN directory tree is not NFS-mounted (or AFS, etc.) from a remote system.
- Ensure that the SATAN directory tree cannot be read by users other than root.
- Do not open any URLs outside your own system and site while running the browser started by SATAN. For example, do not use previously stored URLs such as those found in bookmarks and pull-down menus.
- Do not link to any URLs outside your own system and site while running the browser started by SATAN. If you use external links while SATAN is running from the SATAN browser, security can be compromised on the system from which you are executing SATAN. So, for example, do not use previously stored links such as those found in bookmarks and pull-down menus.

Appendix A: Wietse Venema's PGP Key


```
-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: 2.6


mQCNAirDhV8AAAED/i4LrhQ/mwOgam8ZfQpEcxYoE9kru5oRDGtoVeKae/4bUver
aGX7qVtskD6vwPwr2FF6JW2c+z2oY4JGPGUArORiigoT82/q6vqT0Wm1jIPsXQSB
ZCkBoyvBcmXEi+J7eDBbWLPDxeDimgrORbAIQ4uikRafs8KlpNyA8qbVMny5AAUR
tCV3aWV0c2UgdmVuZW1hIDx3aWV0c2VAd3p2Lndpbi50dWUubmw+
=PQUu

-----END PGP PUBLIC KEY BLOCK-----
```

Appendix B: Tutorial - SATAN Password Disclosure

The following tutorial can be found in
satan-1.1.1/html/tutorials/vulnerability/SATAN_password_disclosure.html

SATAN Password Disclosure

SUMMARY

SATAN password disclosure via flawed HTML clients or environmental problems

IMPACT

Unauthorized users may execute commands through SATAN

BACKGROUND

By default, SATAN runs as a custom HTML (hypertext markup language) server, executing requests from a user-provided HTML browser, or client program. Examples of common HTML clients are Netscape, NCSA Mosaic and Lynx.

An HTML client request is nothing but a network message, and network messages may be sent by any user on the network. To defend itself against requests from unauthorized users, SATAN takes the following precautions:

- SATAN generates a session key, to be used as a secret password, each time it starts up an HTML client. The session key is in the form of a 32-byte quasi-random number. The number is called quasi-random because it is impossible to generate real random numbers using only software.
- SATAN creates HTML files with the secret password embedded in URL (uniform resource locator) links. The HTML file access permissions are restricted to the owner of the SATAN process (and the superuser).
- SATAN rejects HTML requests whose URL does not contain the current SATAN password. This requirement prevents access by unauthorized clients, provided that the current SATAN password is kept secret.

The protection scheme used by SATAN is in essence the same as the scheme used by many implementations of the X Window system: MIT magic cookies. These secrets are normally kept in the user's home directory, in a file called .Xauthority. Before it is granted access to the screen, keyboard and mouse, an X client program needs to prove that it is authorized, by handing over the correct magic cookie. This requirement prevents unauthorized access, provided that the magic cookie information is kept secret.

THE PROBLEM

It is important that the current SATAN password is kept secret. When the password leaks out, unauthorized users can send commands to the SATAN HTML server where the commands will be executed with the privileges of the SATAN process.

Note that SATAN generates a new password every time you start it up under an HTML client, so if you are suspicious, simply restart the program.

SATAN never sends its current password over the network. However, the password, or parts of it, may be disclosed due to flaws in HTML clients or due to weak protection of the environment that SATAN is running in. One possible scenario for disclosure is:

- When the user selects other HTML servers from within a SATAN session, some HTML client programs (Netscape and Lynx) disclose the current SATAN URL, including SATAN password information. The intention of this feature is to help service providers find out the structure of the world-wide web. However, the feature can also reveal confidential information. With version 1.1 and later, SATAN displays a warning when the HTML client program exhibits this questionable (i.e. stupid) feature.

Other scenarios for SATAN password disclosure are discussed in the next section, as part of a list of counter measures.

PREVENTING SATAN PASSWORD DISCLOSURE

The security of SATAN is highly dependent on the security of environment that it runs in. In the case of an X Window environment:

- Avoid using the xhost mechanism, but use xauth and MIT magic cookies or better. Otherwise, unauthorized users can see and manipulate everything that happens with the screen, keyboard and mouse. Of course, this can also be a problem when you are not running the SATAN program at all.

Steps that can help to keep the X magic cookie information secret:

- Avoid sharing your home directory, including .Xauthority file, with other hosts. Otherwise, X magic cookie information may be captured from the network while the X software accesses that file, so that unauthorized users can take over the screen, keyboard and mouse.
- Avoid running X applications with output to a remote display. Otherwise, X magic cookie information can be captured from the network while X clients connect to the remote display, so that unauthorized users can take over the screen, keyboard and mouse.

Finally, steps that can help to keep the current SATAN password secret:

- Avoid sharing the SATAN directories with other hosts. Otherwise, SATAN password information may be captured from the network while the HTML software accesses passworded files, so that unauthorized users can take over the SATAN HTML server.
- Avoid running SATAN with output to a remote display. Otherwise, SATAN password information can be captured from the network while URL information is shown on the remote display, so that unauthorized users can take over the SATAN HTML server.

ADDITIONAL SATAN DEFENSES

The SATAN software spends a lot of effort to protect your computer and data against password disclosure. With version 1.1 and later, SATAN even attempts to protect you after the password has fallen into the hands of unauthorized users:

- SATAN displays a warning and advises the user to not contact other HTML servers from within a SATAN session, when it finds that the HTML client program reveals SATAN password information as part of parent URL information.
- SATAN rejects requests that appear to come from hosts other than the one it is running on, that refer to resources outside its own HTML tree, or that contain unexpected data.
- SATAN terminates with a warning when it finds a valid SATAN password in an illegal request: SATAN assumes the password has fallen into the hands of unauthorized users and assumes the worst.

The CERT Coordination Center staff thanks Wietse Venema for his cooperation and assistance with this revised advisory.

Revision History

```
Sep. 23, 1997 - Updated copyright statement
Aug. 30, 1996 - Information previously in the CA-95.07 and CA-95.07a README
                files was inserted into the advisory.
```