

[NEWS] MacOS X Local SecurityServer Daemon DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0006.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/01/04

To: list@securiteam.com

Date: 1 Jan 2004 18:03:12 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

MacOS X Local SecurityServer Daemon DoS

SUMMARY

SecurityServer is a daemon used by the effected platforms to provide authentication, authorization, password dictionary (Keychain), and other services. It is possible for any user to cause the SecurityServer daemon to crash. When this happens, it will have a cascading effect crashing other processes, and leaving the system in an unusable state.

DETAILS

Vulnerable Systems:

* Apple MacOS X, MacOS X Server, and Darwin.

It is possible to cause the SecurityServer daemon to crash by unlocking a locked keychain and specifying a very long password. When the SecurityServer daemon crashes, it will have a cascading effect crashing other processes that rely on it. Since MacOS X, and many GUI and CLI programs rely on the authentication, authorization, and password dictionary services provided by SecurityServer, this could cause unexpected behavior of those processes.

Securiteam: [NEWS] MacOS X Local SecurityServer Daemon DoS

Typical behavior for programs such as login, sshd, su, and sudo are to prompt the user with 'invalid password' message. Typical behavior for most other applications that use the authorization services is that they will hang. It is not possible to manually restart the SecurityServer daemon unless you already have an existing root shell open before the attack has taken place, since SecurityServer must be launched as root and it does not have the suid bit enabled. Even when it is re-launched after an attack has taken place, it will leave the system in an unusable state. Logins via the GUI (login window) will not work and authorization services will not work either.

The only realistic way to recover from an attack is to reboot the machine. We have not fully investigated the extent that this attack could be exploited, or its effect on a system as a whole since so many programs and applications rely on the SecurityServer daemon.

Vendor Status:

Apple Developer Connection responded that Apple does not give release dates for patches.

Timeline:

??-??-?? Flaw discovered. Most likely in MacOS X Public Beta or 10.0. Matt does not remember the exact date

11-20-03 Vendor is notified of flaw and is supplied with proof of concept code

12-29-03 Asked vendor for status update. Apple Product Security referred me to Apple Developer Connection. Apple Developer Connection informed that Apple does not give release dates for patches

12-30-03 Advisory and proof of concept code released

Recommendation:

As of the release of this advisory Apple has not yet released a patch. We are unable to release a patch because Apple only makes portions of the code needed to build SecurityServer available to the public. The only recommendation is to allow only people you personally trust into effected systems.

Proof Of Concept:

To build this code run: gcc <file name> -framework Security ?-o CrashSecurityServer

```
#include <Security/Security.h>
int main(int argc, const char *argv[])
{
    SecKeychainRef defaultKeychain;
    SecKeychainCopyDefault(&defaultKeychain);
    SecKeychainLock(defaultKeychain);
    SecKeychainUnlock(defaultKeychain, 0xFFFFFFFF, "password", true);
    return 0;
}
```

Securiteam: [NEWS] MacOS X Local SecurityServer Daemon DoS

ADDITIONAL INFORMATION

The information has been provided by
<mailto:marukka@consoleconductor.com> Matt Burnett

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.