

[UNIX] Clam AntiVirus ClamAV CAB File Unstore Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00044.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 26 Apr 2007 14:28:03 +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>

Clam AntiVirus ClamAV CAB File Unstore Buffer Overflow Vulnerability

SUMMARY

<<http://www.clamav.net/>> Clam AntiVirus is "a multi-platform GPL anti-virus toolkit. ClamAV is often integrated into e-mail gateways and used to scan e-mail traffic for viruses. Cabinet, or CAB, files are the Microsoft Windows native format for storing compressed archives".

Remote exploitation of a buffer overflow vulnerability in Clam AntiVirus' ClamAV allows attackers to execute arbitrary code with the privileges of the affected process.

DETAILS

Vulnerable Systems:

- * ClamAV versions 0.90rc3 through 0.90.1.

Immune Systems:

- * ClamAV version 0.90.2

The vulnerability exists within the `cab_unstore()` function in `libclamav`, the library used by `clamd` to scan various file types. A 32-bit signed

[UNIX] Clam AntiVirus ClamAV CAB File Unstore Buffer Overflow Vulnerability

integer is taken from the packet and compared against the sizeof() the destination buffer. However, the sizeof() return value is improperly casted to a signed integer. By supplying a negative value, an attacker can pass cause the comparison to succeed. This eventually leads to an exploitable stack-based buffer overflow.

Successful exploitation of this vulnerability results in code execution with the privileges of the process using libclamav.

In the case of the clamd program, this will result in executing code with the privileges of the clamav user. Unsuccessful exploitation results in the clamd process crashing.

This vulnerability only exists in the recent 0.9x versions of ClamAV. As such, the vulnerable code is not present in the versions distributed with Red Hat Enterprise or other open source distributions.

Vendor Status:

The ClamAV team has addressed this vulnerability within version 0.90.2.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1997>>
CVE-2007-1997

Disclosure Timeline:

- * 04/05/2007 – Initial vendor notification
- * 04/06/2007 – Initial vendor response
- * 04/16/2007 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=513>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=513>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

[UNIX] Clam AntiVirus ClamAV CAB File Unstore Buffer Overflow Vulnerability

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.