

n.runs AG
http://www.nruns.com/
n.runs-SA-2007.025

security(at)nruns.com
24-Aug-2007

Vendor: ClamAV, <http://www.clamav.net>
Affected Products: ClamAV, <http://www.clamav.net>
Vulnerability: Remote Code Execution
Risk: MEDIUM

Vendor communication:

20070810 Initial notification to ClamAV
20070810 ClamAV Responses
20070810 PoC files sent to ClamAV
20070821 ClamAV releases version 0.91.2
20070822 n.runs AG releases a coordinated disclosure advisory

Overview:

Clam AntiVirus is an open source (GPL) anti-virus toolkit for UNIX, designed especially for e-mail scanning on mail gateways. It provides a number of utilities including a flexible and scalable multi-threaded daemon, a command line scanner and advanced tool for automatic database updates. The core of the package is an anti-virus engine available in a form of shared library.

Description:

A remotely exploitable vulnerability has been found in clamav-milter when used with sendmail. In detail, the following flaw was determined:

- Arbitrary code execution due to insecure call to popen()

Impact:

This vulnerability can lead to remote code execution with root privileges. Leading to a complete compromise of the vulnerable system. An attacker can inject shell commands into the recipient field of sendmail, if clamav-milter was started with the black hole mode activated.

The vulnerability is present in at least clamav version 0.91.1, prior versions may also be affected.

Solution:

A new stable release (clamav 0.91.2) is available at the clamav website which fixes the vulnerability.

Credit:

Bugs found by Nikolaos Rangos of n.runs AG.

References:

<http://www.clamav.net/download/sources>

This Advisory and Upcoming Advisories
http://www.nruns.com/security_advisory.php
<http://www.nruns.com/parsing-engines-advisories.php>

Unaltered electronic reproduction of this advisory is permitted. For all other reproduction or publication, in printing or otherwise, contact securitynruns.com for permission. Use of the advisory constitutes acceptance for use in an as is condition. All warranties are excluded. In no event shall n.runs be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if n.runs has been advised of the possibility of such damages.

Copyright 2007 n.runs AG. All rights reserved. Terms of apply.