

[NT] Servers Alive Privilege Escalation Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0080.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/17/05

To: list@securiteam.com

Date: 17 Mar 2005 11:11:46 +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>

Servers Alive Privilege Escalation Vulnerability

SUMMARY

" <<http://www.woodstone.nu/salive/index.asp>> Servers Alive is an end-to-end network monitoring tool. It works agentless and across operating systems. Its checks and alerts are on the cutting edge of technology. It allows you to easily monitor hundreds of servers, or Internet services on a server, for uptime and availability. When it detects that a monitored service or computer has gone down it can make you aware through a variety of means."

A privilege escalation vulnerability has been discovered in Servers Alive, allowing a local non-privileged user to obtain SYSTEM privileges.

DETAILS

Vulnerable Systems:

* Servers Alive versions 4.1 and 5.0

Servers Alive can be run in two modes: as an application or as a service. When run as a service, the application is permitted to interact with the desktop and runs under the context of SYSTEM. When clicking the 'Local

Securiteam: [NT] Servers Alive Privilege Escalation Vulnerability

manual' under help, the application does not drop privileges.
Consequently, it is possible to assume SYSTEM privileges by:

- 1) Viewing the source of the help file, which opens in Notepad
- 2) In Notepad, selecting File, Open
- 3) Launching a system utility such as cmd.exe.

Workaround:

- * Only allow trusted users with Administrator-level privileges to logon interactively.
- * Physically secure the server on which the application is installed.
- * Do not run the application as a service.

Disclosure Timeline:

- * 01.24.05 – Vendor notified.
- * 01.25.05 – Vendor responded, discussion ensued.
- * 01.29.05 – CERT notified
- * 02.18.05 – CVE Candidate Number assigned from CERT
- * 03.15.05 – Advisory publicly released

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0352>>
CAN-2005-0352

ADDITIONAL INFORMATION

The information has been provided by <mailto:secure@michaelstarks.com>
Michael Starks.

=====

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.