

[NEWS] Lotus Domino Bindsock Notes_ExecDirectory Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0129.html>

From: support@securiteam.com

Date: 04/30/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 30 Apr 2002 22:41:38 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Lotus Domino Bindsock Notes_ExecDirectory Buffer Overflow Vulnerability

SUMMARY

Lotus Domino bindsock is vulnerable to a buffer overflow condition that allows a local attacker to gain root privileges. The problem is due to insufficient bounds checking for the Notes_ExecDirectory environment variable. An attacker can use a string for Notes_ExecDirectory that, when processed, will execute arbitrary code.

DETAILS

Vulnerable systems:

- * Lotus Domino 5.0.4 on Linux
- * Lotus Domino 5.0.4a on Linux
- * Lotus Domino 5.0.5 on Linux
- * Lotus Domino 5.0.6 on Linux
- * Lotus Domino 5.0.6a on Linux
- * Lotus Domino 5.0.7 on Linux
- * Lotus Domino 5.0.7a on Linux
- * Lotus Domino 5.0.8 on Linux
- * Lotus Domino 5.0.9 on Linux

Securiteam: [NEWS] Lotus Domino Bindsock Notes_ExecDirectory Buffer Overflow Vulnerability

Immune systems:

- * Lotus Domino 5.0.9a on Linux

Technical Recommendation:

Upgrade with the latest version available. Lotus Domino version 5.0.9a is not vulnerable to the issue.

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:researchteam5@esecurityonline.com>> researchteam5.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] Lotus Domino Bindsock Arbitrary File Creation Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)