

[NT] iPlanet Messaging Server Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-09/0014.html>

From: support@securiteam.com

Date: 09/03/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] iPlanet Messaging Server Buffer Overflow Vulnerability

Message-Id: <20010903195819.0E1E6138C0@mail.der-keiler.de>

Date: Mon, 3 Sep 2001 21:58:19 +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.

iPlanet Messaging Server Buffer Overflow Vulnerability

SUMMARY

Netscape Administration Server, provided by iPlanet Messaging Server as a console program for administration, suffers from a buffer overflow vulnerability. The vulnerability allows remote users to execute arbitrary commands with SYSTEM privilege.

DETAILS

Vulnerable systems:

iPlanet Messaging Server version 5.1 (Winnt)

iPlanet Messaging Server is designed to provide SMTP, IMAP4, POP3 and Web-based mail services. Basic authorization is required for editing of user information, therefore a supplied username and password are sent to the server after being base64 encoded. If long strings are included in username, ns-admin.exe will overflow. The overflow will allow remote users to execute arbitrary commands with SYSTEM privilege.

Solution:

Securiteam: [NT] iPlanet Messaging Server Buffer Overflow Vulne

It is strongly recommended that you set up access control of Administration Server to deny access to servers to untrusted users.

ADDITIONAL INFORMATION

The information has been provided by <mailto:snsadv@lac.co.jp> SNS Team of LAC.

=====

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: "[\[UNIX\] LPRng/rhs-printfilters Vulnerability Leads to Remote Execution of Commands](#)"
 - **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)