



IDP

Release Notes

Release 3.2r4a

06-05-2007

Contents

- 1 Version Summary on page 2
- 2 New Features on page 2
- 3 Changes to Default Behavior on page 2
- 4 Addressed Issues on page 2
- 5 Known Issues on page 2
 - 5.1 Limitations of Features on page 3
 - 5.2 Compatibility Issues on page 3
 - 5.3 Known Issues on page 3
- 6 Installing the Update on page 5
- 7 Getting Help on page 6

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1857-000

1 Version Summary

This release contains updates for the IDP 3.2 software release.

2 New Features

- None.

3 Changes to Default Behavior

- None.

4 Addressed Issues

The following issues are addressed in this release:

- UTF-8 parser update -- HTTP content scanning system full-width/half-width Unicode encoding bypass. Various HTTP content scanning systems fail to properly scan full-width/half-width Unicode traffic. This can allow malicious HTTP traffic to bypass content scanning systems.

Full-width and half-width encoding is a technique for encoding Unicode characters. Various HTTP content scanning systems fail to properly scan full-width and half-width Unicode encoded HTTP traffic. By sending specially-crafted HTTP traffic to a vulnerable content scanning system, an attacker may be able to bypass that content scanning system

Public announcement of this issue:

<http://www.kb.cert.org/vuls/id/739224>

- cs11299—Issue with SSL decoder.
- cs11064—Issue with SMTP decoder.

5 Known Issues

This section describes known issues with the current release.

Section 5.1 “Limitations of Features” identifies features that are not fully functional at the present time, and are not supported for this release.

Section 5.2 “Compatibility Issues” describes known compatibility issues with other products, including but not limited to specific Juniper Networks’ appliances, Internet browsers, and other vendor devices. Whenever possible, information is provided for ways to avoid the issue, minimize its impact, or in some manner work around it.

Section 5.3 “Known Issues” describes deviations from intended product behavior in IDP as identified by Juniper Test Technologies through their verification procedures. Whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

5.1 *Limitations of Features*

- None.

5.2 *Compatibility Issues*

- None.

5.3 *Known Issues*

The following are known deficiencies at the time of this release. Whenever possible, a work-around is suggested following the description of the problem. Workaround information starts with “W/A:”.

- cs11816—IDP drops the ACKs to the data sent from the other end during the TCP half-close state.

W/A: Contact JTAC for a patch.

- cs10915: The quad card “Intel[R] PRO/1000 GT QUAD PORT Server Adapter” is not compatible with IDP Sensors. With the Intel[R] PRO/1000 GT QUAD PORT Server Adapter installed in the sensor, error messages appear when the kernel module is getting started. The drivers used by the Sensors do not support this quad card. Only applies to IDP 100, 500, and 1000.

W/A: Download and install the IDP Quad Port Ethernet driver from the Juniper web site prior to installing the card. The driver can be found under Download Software -> IDP software -> 3.2 or 4.0 download pages. Review the IDP Quad Port Ethernet Driver Update document for installation instructions.

- cs10138: Updating attack objects may create an exempt all attacks rule if the referred signature (in exempt rule) is removed from attack db.

W/A: Check the Exempt Rule after every attack update.

- cs10068: Management Server: mLogPurger line 391: [too many arguments]. If the filesystem is installed using LVM (Logical Volume Manager), the OS returns unexpected values for commands like 'ls -l'. As a result, IDP functions that check the filesystem will throw errors because of the unexpected return value.

W/A: Reformat the filesystem as ext3 and this will resolve the issue.

- cs8611: IDP Scheduler fails to run automatically when the DISPLAY is defined as :5.0.

W/A: Export the DISPLAY environment variable as IP_Address:6.0.

- cs8123: IDP standalone HA failover times varies as the IDP does not send gratuitous ARP.

- cs7965: The Source and destination IP Address are swapped for the log that detects the "HTTP Invalid: Invalid Value in Header Field" attack.

- cs7922: Maximum policy versions that can be stored are 999.

W/A: Select the Policy and Save As a new policy and update the new policy to the device when the policy versions reach 999.

- cs7949/cs7664: Attack Object version is not updated when the signatures are updated using Local.

- cs7896: Unable to delete an object from a custom static group.

- cs7644 — Attack Update window not displayed correctly when "emulate Windows XP" is selected from "Tools > Preferences > Look & feel" tab.

W/A: Don't select "Emulate Windows XP" look & feel option.

- cs7284: During attack objects update, manual update may not work properly. Deselecting the Signatures marked for modification or deletion may still modify or delete them.

W/A: Perform the manual attack objects update and check for any particular signature that you do not want to be modified or deleted. Now cancel the update, create a custom signature of the signature to be saved and then do an attack objects update.

- dp04794: May get 'relocation error:' on console while upgrading:

sleep: relocation error: /lib/i686/libpthread.so.0: undefined symbol: _dl_cpuct

W/A: Ignore the message. It does not affect the runtime behavior of the Sensor.

- dp04427: A few smb-dce-rpc (smb-dce-rpc-bind-ack & smb-dce-rpc-request) contexts may not trigger.

- dp04416: apache modulearg errors seen while saving config from ACM.

W/A: Ignore these messages. They are harmless and do not affect any functionality of the Sensor.

- dp04355: With Solaris Management Server, UI hangs on accessing logviewer.

W/A: Restart Management Server.

- dp04347: Sensor not displayed in UI under device monitor on Solaris 8 Management Server.

W/A: Use Solaris 9 or Linux Management Server.

6 Installing the Update

Upgrade to 3.2r4a is supported only from 3.2r4 release.

You must upgrade the IDP system components in the following order:

1. Upgrade the IDP Sensor software.
2. (IDP 100, 500, 1000 only) If you have an Intel[R] PRO/1000 GT QUAD PORT Server Adapter in your Sensor, you must reinstall the IDP Quad Port Ethernet driver. The driver is available from the Juniper web site under Download Software -> IDPsoftware -> 3.2 or 4.0 download pages. Review the IDP Quad Port Ethernet Driver update document for installation instructions.
3. Update attack objects.

For detailed information on upgrading IDP software, see the *IDP Upgrade Guide*.

7 Getting Help

For more assistance with Juniper Networks products, visit:

www.juniper.net/support

Juniper Networks occasionally provides maintenance releases (updates and upgrades) for ScreenOS firmware. To have access to these releases, you must register your NetScreen device with Juniper Networks at the above web address.

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.
ATTN: General Counsel
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
U.S.A.

www.juniper.net

Writer: Mark Schlagenhauf