



IDP

Release Notes

Release 3.2r3

8-22-06

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 3
 - 5.1 Limitations of Features on page 3
 - 5.2 Compatibility Issues on page 4
 - 5.3 Known Issues on page 4
- 6 Installing the Update on page 5
- 7 Getting Help on page 7

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1829-000, Rev. B

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:

- 10070: IDP does not block multicast traffic in STP blocking port state.
- 9711: Missing identification of Japanese character set resulting in false positive in SMTP.
- 9665: False positives for MSRPC:Response without a Request anomaly.
- 9458: Stack overflow while verifying yahoo messenger status code.
- 9410: IDP Manager 3.1r4 does not support multi-language environment.
- 9063: RADIUS authentication fails for user authentication when accessing ACM.
- 8763: Policy compile only works on one half of cluster.
- 8438: ACM required config to be saved even though ACM configuration was not changed.
- 7940: False positive on SMTP: Invalid Filename Protocol anomaly.
- 7914: The log2action generates mis-formatted CSV file when the attack log for the "HTTP:OVERFLOW:CONTENT-OVERFLOW" attack object is present.
- 7824: On Solaris Management Server, Profiler fails to properly sync with the IDP Manager.
- 7526: Busy processor caused NIC Bypass to kick in inappropriately.
- 7394: Coredump due to Yahoo Messenger traffic issue.
- 7253: Exporting HTML shows "NULL" IP address entry in custom report.
- 7076: In sniffer mode ACM does not reconfigure TCP reset back to default.
- 6705: Forwarding interfaces auto-negotiating even when set to specific speed/duplex settings.

- dp04428: smb-connect-service context is not generated.
- dp04361: PCRE code causes a crash when certain signatures are used with matching traffic. (Example: HTTP:STC:IE:IFRAME-NAME-OF)
- dp04360: Attack not detected in reordered fragment traffic.
- dp04354: IDP stack retraced on replay of a PCAP that generates ftp:overflow:line-to-long
- dp04222: IDP crashed while decoding HTTP traffic.
- dp04121: Multiple responses in one packet with header flags triggers False Positive for 'Netbios NS: Short Message'.
- dp04004: False Positive on VOIP:SIP:BAD-VERSION since case sensitivity was ignored.
- dp03856: ACM configuration caused error messages with Peer Port Modulator.
- dp03513: pkid process terminates overnight.
- dp03319: The 'CHAT:IRC:OVERFLOW:CHANNEL' is reported for false positive. Should account for " ' " separated multi-channels.
- dp03266: The context ftp-reply-500-line is triggered instead of ftp-reply-200-line, and vice-versa.
- dp03152: Support for FTP evasion techniques can be added in IDP.

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:".

- 10915: 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.

- 10138: 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.

- 10068: Mgmt 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.

- 8611: 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.

- 8123: IDP standalone HA failover times varies as the IDP does not send gratuitous ARP.
- 7965: The Source and destination IP Address are swapped for the log that detects the "HTTP Invalid: Invalid Value in Header Field" attack.
- 7922: 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.

- 7949/7664: Attack Object version is not updated when the signatures are updated using Local.
- 7896: Unable to delete an object from a custom static group.
- 7644 — 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.

- 7284: During attack objects update, manual update may not work properly. Unchecking 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.

- 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 Mgmt Server.

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

- dp04344: May get the following 'relocation error:' on console while upgrading sensor to 3.2r3:

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

W/A: Ignore the message. This message is not harmful and does not affect any functionality of the Sensor.

6 Installing the Update

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

1. Upgrade the IDP Sensor software
2. Upgrade the IDP Management Server software
3. Upgrade the IDP UI software
4. Update attack objects

Use the following files to upgrade your system. You can also use these files to do new installations:

- sensor_3_2r3.sh: Sensor upgrade/installation script

- `mgtsvr_linux_3_2r3.sh`: Management Server upgrade/installation script, Linux version
- `mgtsvr_solaris_3_2r3.sh`: Management Server upgrade/installation script, Solaris version
- `install_3_2r3.exe`: UI upgrade/installation script, Windows version
- `install_3_2r3.bin`: UI upgrade/installation script, Linux version
- `install_scheduler_3_2r3.bin`: IDP Scheduler, Linux version. See the *IDP Concepts and Examples Guide* for more information.

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

