Internet Draft: Notify Mail
Document: draft-gellens-notify-mail-02.txt
Expires: July 2005

R. Gellens
QUALCOMM

January 2005

Simple New Mail Notification

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of RFC 3668.

By submitting this Internet-Draft, I accept the provisions of Section 3 of RFC 3667 (BCP 78).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.

Abstract

This memo documents a long-standing technique, supported by a large number of mail servers, which allows users to be notified of new mail. In addition to server support, there are a number of clients which support this, ranging from full email clients to specialized clients whose only purpose is to receive new mail notifications and

alert a mail client.

In brief, the technique is for the server to send the string "nm_notifyuser" CRLF to the finger port on the IP address (either configured or last used) for the user who has received new mail.

Table of Contents

1. Introduction 3
2. Conventions Used in this Document 3
3. Simple Mail Notification 3
4. Example 4
5. Security Considerations 4
6. IANA Considerations 5
7. Acknowledgments 5
8. Normative References 5
9. Informative References 5
10. Author's Addresses 5
Intellectual Property Statement 5
Full Copyright Statement 6
Disclaimer 6

1. Introduction

There is a long-standing technique supported by a large number of mail servers which allows users to be notified of new mail. In addition to server support, there are a number of clients which support this, ranging from full email clients to specialized clients whose only purpose is to receive new mail notifications and alert a mail client. This technique is sometimes known as "notify mail" (after a shareware client of the same name), sometimes called "biff", and sometimes the "finger hack".

2. Conventions Used in this Document

In examples, "C:" is used to indicate lines sent by the client, and "S:" indicates those sent by the server. Line breaks within a command example are for editorial purposes only. Line breaks in the protocol are indicated by "CRLF".

3. Simple Mail Notification

The technique is for the server to send the string "nm_notifyuser" immediately followed by CRLF to the finger port on the IP address for the user who has received new mail. The finger port is 79. (Note that only the port for finger is used; the finger protocol itself is not used.)

The IP address to use may be configured, or the server may use the IP address that was last used to check mail by the user. Typically this is a per-account configuration option.

To be useful, on the client system a process must be listening to the finger port. When it receives the "nm_notifyuser" string, it takes a configured action, typically instructing a mail client to fetch mail.

Normally, a TCP connection to the target computer is opened, the "nm_notifyuser" string is sent, and the connection is closed without waiting for any response.

In some cases UDP is used instead of TCP, but the default and general practice is TCP. Even though one a single message in one direction is sent (with no reply), TCP is used most often, probably for reliability.

There is an assumption that the client listening on an IP address only has responsibility for one email account; if a client can check multiple accounts and receives the "nm_notifyuser" string, it does not know which account received the mail.

There is a requirement that a finger daemon is not active on the client.

4. Example

This example assumes that new mail has arrived at server mail.isp.example.com for account fastness@example.net. The server has determined an IP address to which notification should be sent.

```
C: <listens on TCP port 79>
S: <opens TCP connection to IP address port 79>
C: <accepts inbound connection on port 79>
S: nm_notifyuserCRLF
S: <closes TCP connection>
```

5. Security Considerations

There is of course no assurance that the "nm_notifyuser" message is being sent to the correct IP address. Nor does the listening agent on the client system have any assurance that a "nm_notifyuser" string was sent by a mail server which has received new mail for the user.

It is trivial for an attacker to send large numbers of "nm_notifyuser" messages to any targeted system. Client systems listening for this message SHOULD implement protections against being flooded with notifications. Many server systems already implement protections against users logging in and checking mail too

frequently.

Since use of this protocol requires that a port be open with an agent listening on it, if that agent contains vulnerabilities it may create a remotely exploitable attack (for example, buffer overflows permitting an attacker to execute arbitrary code on the client system with the permissions of the agent). As usual with a process listening on a port, the process should execute with the least possible privelege level and access.

6. IANA Considerations

The notify mail hack (and this document) should be included as an additional usage for port 79.

7. Acknowledgments

The NotifyMail shareware utility was written by Scott Gruby.

8. Normative References

None.

9. Informative References

None.

10. Author's Addresses

Randall Gellens
QUALCOMM Incorporated
6455 Lusk Blvd.
San Diego, CA 92121-2779
USA
randy@qualcomm.Com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that

it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Full Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Disclaimer

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.