[Bug 6496] New: Message-Id leaks current user/hostname of the Java process (security)

bugzilla-daemon@kenai.com <bugzilla-daemon@kenai.com> Wed, Aug 6, 2014 at 1:41 AM
To: _ikki@kenai.com

Bug ID	6496
Summary	Message-Id leaks current user/hostname of the Java process (security)
Product	javamail
Version	1.5.3
Hardware	All
OS	All
Status	NEW
Severity	normal
Priority	P5
Component	internet
Assignee	shannon@kenai.com
Reporter	_ikki@kenai.com
CC	issues@javamail.kenai.com

JavaMail uses the following method to set the Message-Id of outgoing messages:

javax.mail.internet.MimeMessage:
setHeader("Message-ID", "<" + UniqueValue.getUniqueMessageIDValue(session) +
">");

where getUniqueMessageIDValue() is generated by using:

InternetAddress addr = InternetAddress.getLocalAddress(ssn);
...
suffix = addr.getAddress();

According to http://tools.ietf.org/html/rfc2392, "the originator of a message
using mid and cid URLs must take precautions to insure that confidential
information is not disclosed."

Instead, JavaMail is leaking the process's user and machine hostname.

E.g. 488461919.0.1407279230343.JavaMail.luca@myMac.local

In case of services using JavaMail to send emails (registration forms, etc.), this can facilitate further attacks such as SSH bruteforcing - since the attacker has obtained knowledge of both hostname and a valid user.

As for RFC2392, the only requirement for message-id and content-id is that they must be globally unique.

E.g. Gmail uses something like
Message-ID: <CACbf...GqiZ5wEuW40hwMPPxA@mail.gmail.com>