

[NEWS] JavaMail Information Disclosure (msgno)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0113.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/19/05

To: list@securiteam.com

Date: 19 May 2005 16:15:21 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

JavaMail Information Disclosure (msgno)

SUMMARY

"The <<http://java.sun.com/products/javamail/>> JavaMail API provides a platform-independent and protocol-independent framework to build mail and messaging applications. The JavaMail API is implemented as a Java platform optional package and is also available as part of the Java 2 platform, Enterprise Edition. JavaMail provides a common, uniform API for managing electronic mail. It allows service-providers to provide a standard interface to their standards-based or proprietary messaging systems using the Java programming language. Using this API, applications access message stores, and compose and send messages. The JavaMail API is composed of a set of abstract classes that model the various pieces of a typical mail system."

The JavaMail API doesn't properly validate authenticated user message number attribute, allowing authenticated users to view other's messages.

DETAILS

Vulnerable Systems:

- * Solstice Internet Mail Server POP3 2.0
- * JavaMail API

Securiteam: [NEWS] JavaMail Information Disclosure (msgno)

The JavaMail API doesn't properly validate authenticated user message number attribute in MimeMessage constructor javax.mail.internet.InternetHeaders object, authenticated user is being able to access to others message requesting msgno. First attacker need to login to javamail from web with correct user name and password. Then the attacker will be able to request others message through msgno. Which means the attacker will be able to view all message from server.

The MimeMessage constructor holds its headers in javax.mail.internet.InternetHeaders object. This object, when constructed with an InputStream, reads lines from the stream until it reaches the blank line that indicates end of header. It stores the lines as RFC822 header-fields. After the InternetHeaders object reads from the input stream, the stream is positioned at the start of the message body.

The POP3 implementation uses this constructor to load the message headers when one is requested:

```
public class POP3Message extends MimeMessage {
//Keep track of whether the Message data has been loaded
boolean loaded = false;
int hdrSize;
..
public String[] getHeader(String name) {
//Get the headers on demand from the message store
load();
// Don't need to reimplement getting the header object's contents
return super.getHeader(name);
}
/** Reimplement all variants of getHeader() as above */
..
private synchronized void load() {
if (!loaded) {
// Get message data (headers and content) and cache it
content = POP3Command("RETR", msgno);
// Open a stream to the cache
InputStream is = new ByteArrayInputStream(content);
// Setup "headers" field by getting the header data
headers = new InternetHeaders(is);
// Save header size to easily access msg content from cache
hdrSize = content.length - is.available();
loaded = true;
}
```

This line make authenticated user to able to view others message through msgno :

```
content = POP3Command("RETR", msgno);
```

When user login and view his message and he may notice that <http://javamaildomain.com/ReadMessage.jsp?msgno=1000>

User can do easily change msgno to whatever he want. If he entre valid message no, then he will be able to view others message.

Securiteam: [NEWS] JavaMail Information Disclosure (msgno)

<http://javamaildomain.com/ReadMessage.jsp?msgno=10001>

<http://javamaildomain.com/ReadMessage.jsp?msgno=10002>

Will not be his message number. And now user may know that he is accessing others message.

ADDITIONAL INFORMATION

The information has been provided by <mailto:ygnboyz@gmail.com> Thet Aung Min Latt.

=====

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.