

MWR InfoSecurity Advisory

CommuniGate Pro -
Webmail XSS Session Hijacking
Vulnerability

27th February 2007

MWR  INFOSECURITY

INDEX

1. Detailed Vulnerability description	4
1.1. Introduction	4
1.2. Overview of Vulnerability	5
1.3. Exploit Information	6
1.4. Recommendations	7

CommuniGate Pro – Webmail XSS Session Hijacking Vulnerability

CVE Reference: Not yet submitted

Date: 2007-02-27

Severity: High Risk

Local/Remote: Remote

Vulnerability Class: XSS / Information Disclosure

Vendor URL: www.communiGate.com

Vendor Response: A fix has been implemented for version 5.1.7

Exploit Details Included: Yes

OWASP Designation: Cross Site Scripting (A4)

Web Application Language: Custom/Unknown

Affected versions: 5.1.X up to and including 5.1.6.

Impact: The vulnerability potentially allows for a user's session to be hijacked and for other malicious scripts to be executed within the context of the user's browser window.

Overview: The CommuniGate Pro application provides a web based application allowing users to retrieve emails using a web browser. However, email content is not sufficiently sanitised and can result in the execution of arbitrary scripts. On accessing the web interface of the application the user is assigned a session ID, by sending a specially crafted email an attacker would be able to trick the user into transmitting their session ID to the attacker. The vulnerability affects the majority of the skins available for the application.

CommuniGate have confirmed that the following skins are affected:

- GoldenFleece
- Simplex
- Viewpoint
- Aquinox
- Overview
- XChange

Cause: The vulnerability is the result of insufficient sanitisation of email content when the user chooses to reply to an email. Some areas of the application safely display potentially malicious content and JavaScript without first executing it. However, on choosing to reply to an email, scripts contained within the email being replied to are interpreted by the browser giving an attacker a vector for performing XSS attacks.

Interim Workaround: It should be ensured that the "Fixed Address Check" option is not disabled unless essential and particular caution should be taken when replying to all messages. This check ensures that a user's session is only ever accessible from a single IP address and may help prevent session hijacking. Additionally users should ensure that they correctly log out of the application on exiting and that one of the unaffected skins is used.

Solution: CommuniGate have addressed this issue and implemented a fix in version 5.1.7 with reference "Bug Fix: WebSkins: 5.1c3". Version 5.1.7 can be downloaded from the following location:

<ftp://ftp.communiGate.com/pub/CommuniGatePro/5.1>

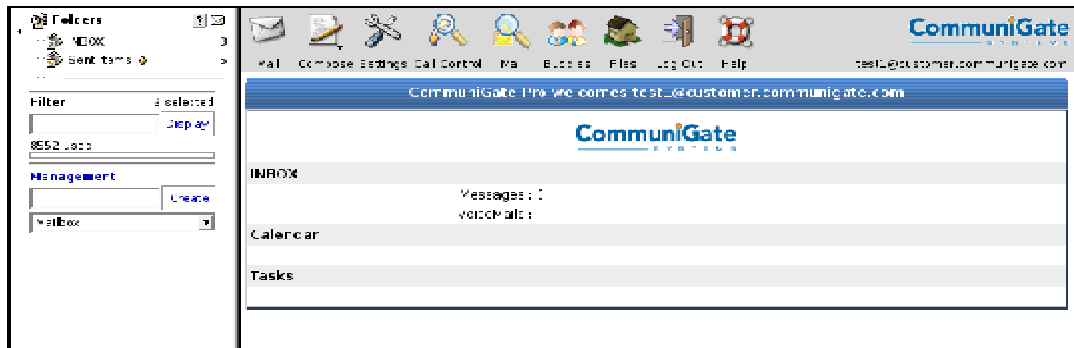
Section 1.4 contains further platform specific URLs where the latest release can be obtained.

1. Detailed Vulnerability description

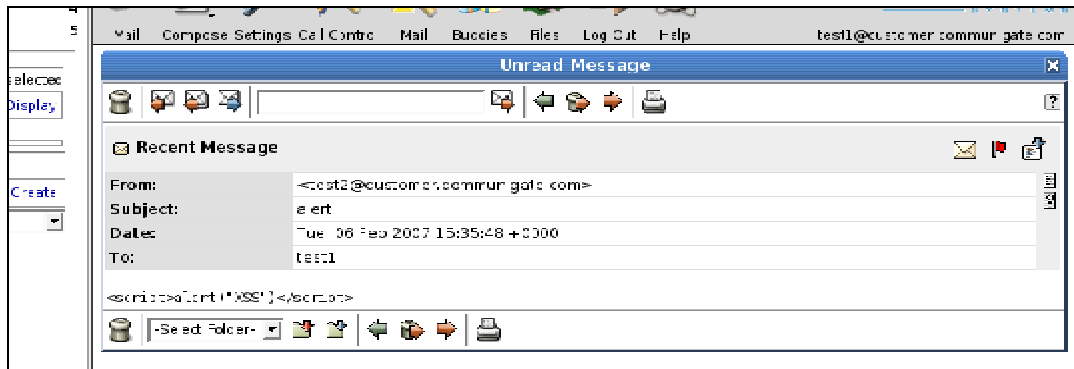
1.1. Introduction

CommuniGate Pro is an Internet based communications server with a large amount of functionality. The vulnerability reported here affects the web interface provided to users in order to perform tasks such as sending and receiving email. The application is available for most widely deployed operating systems.

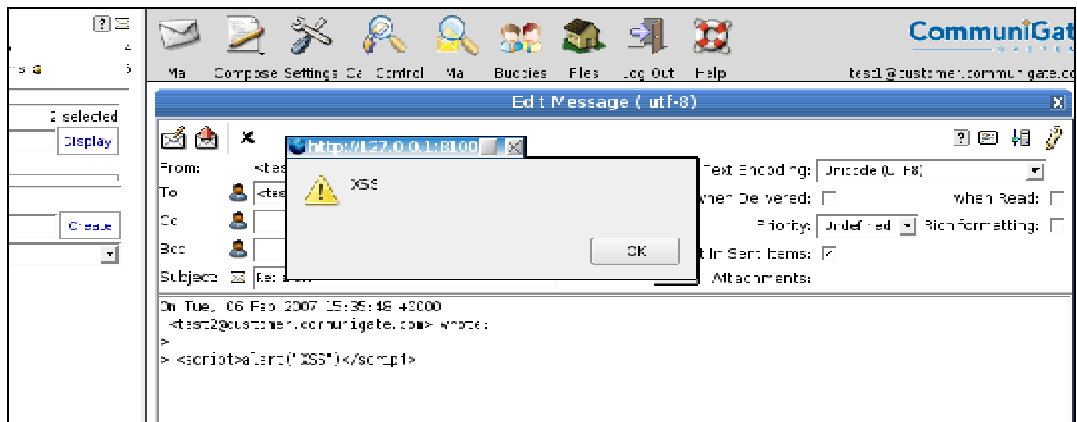
The web interface is shown in the following screenshot and enables a user to perform several tasks including sending and receiving emails:



The following screenshot shows an email message containing some JavaScript which if interpreted by the users browser will render an alert box to the screen containing the text XSS.



Displaying this message does not result in the JavaScript being executed by the browser, however on selecting the 'Reply' or 'Reply to all' options the JavaScript is interpreted by the browser and results in its execution as is shown in the next screenshot.



Within the application a user is bound to a session ID which acts as a mapping to the users account and passed within the GET request. An example URL is shown below:

<http://www.example.com/Session/9-CS6Tt1kjGCav2Hcz4ciY/frameset.wssp?>

Thus, by obtaining this URL an attacker would be able to gain access to the account of the user. This can be achieved by using the XSS vulnerability described above to transmit the current URL to a remote location. There is a measure in place to mitigate this, the application ties a session to an IP address by default, however, this can be disabled and with a large number of people accessing the Internet through a NATted environment or through a proxy it does provide a level of security but not sufficient to completely mitigate this attack.

1.2. Overview of Vulnerability

The vulnerability arises due to lack of sanitisation of email content and an example exploit is described below. The attack described exploits the vulnerability in order to obtain copies of all emails stored within the user's inbox.

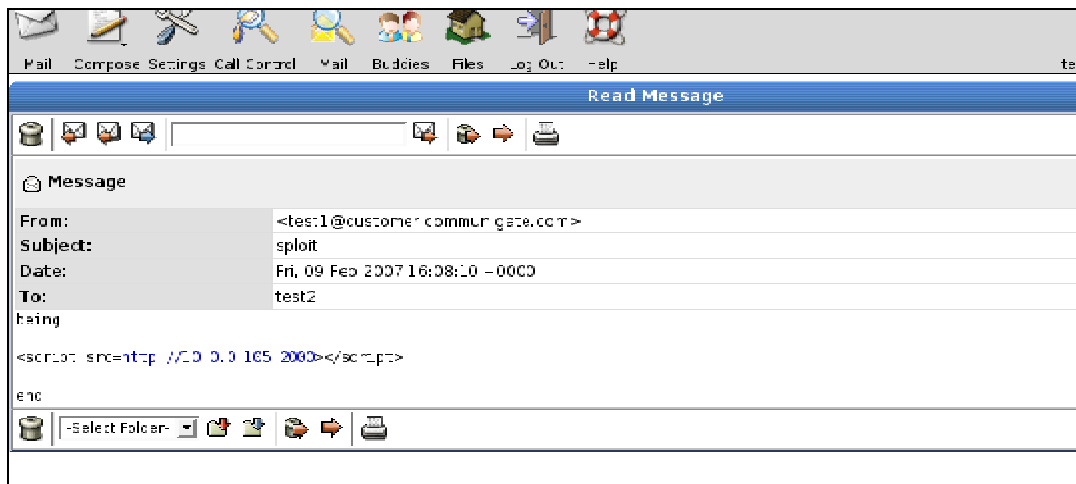
The attack described in the following section is performed in the following steps:

1. An email containing the XSS is sent to a user. In order to increase the chances of success the email may appear to come from a mailing list and request that the user replies to the email in order not to receive any further emails from the organisation.
2. A server is set up to listen for requests sent by the targeted user's browser when the script embedded in the email is executed.
3. The user hits the reply button within the web interface (although is not required to actually reply to the email) and the script is executed.
4. The server set up by the attacker receives the request from the script and manipulates the referrer URL so that it points to the user's inbox.
5. A script running on the attacker's server sends requests to the CommuniGate server iterating through the users inbox downloading their emails.

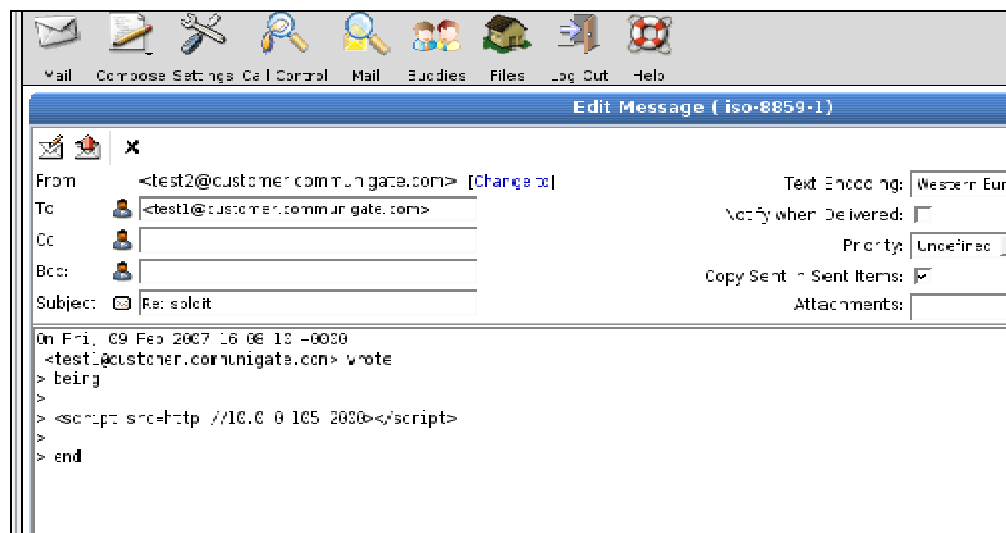
The scope of attacks which can be performed through this vulnerability is huge and this attack (described in full detail in the next section) is described as a proof of concept only.

1.3. Exploit Information

Firstly an email is sent out to the target. In this example the email sent out is shown below in the targets inbox:-



JavaScript has been embedded within the email body. This JavaScript makes a request to the server 10.0.0.105, port 2000. In order for this script to be executed the user must choose to reply to the email. On doing this the user sees the following:-



To the user this appears as expected and there is no indication that the script has been interpreted unless the user is paying particularly sharp attention to their status bar. However the JavaScript has resulted in a request being made to a webserver which has taken the referrer URL, which in this case is:

```

http://127.0.0.1:8100/Session/9-
CS6Tt1kjGCav2Hcz4ciY/compose.wssp?OrigMessage=3&OrigMailbox=INBOX&Operation=Reply&
    
```

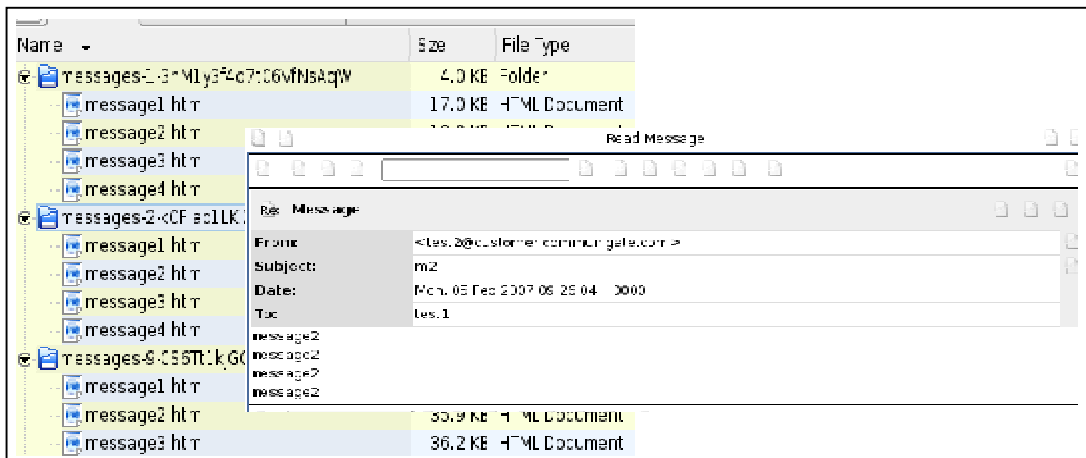
It then manipulates the URL to create the following URL:

<http://127.0.0.1:8100/Session/9-CS6Tt1kjGCav2Hcz4ciY/Message.wssp?Mailbox=INBOX&MSG=1>

This new URL is a direct link to the user's inbox. The querystring contains the number of the message in the inbox, a script on the server runs iterating through downloading messages from the users inbox to the server until there are no more messages left. A server was written to perform receive the XSS requests manipulate the referrer and download the contents of the users inbox. The output of the server is shown below:-

```
>>> got referer http://127.0.0.1:8100/Session/9-
CS6Tt1kjGCav2Hcz4ciY/compose.wssp?OrigMessage=3&OrigMailbox=INBOX&Operation=Reply&
>>> Built new URL: http://127.0.0.1:8100/Session/9-
CS6Tt1kjGCav2Hcz4ciY/Message.wssp?Mailbox=INBOX&MSG=1
>>> pulling down messages...
GET /Session/9-CS6Tt1kjGCav2Hcz4ciY/Message.wssp?Mailbox=INBOX&MSG=1
GET /Session/9-CS6Tt1kjGCav2Hcz4ciY/Message.wssp?Mailbox=INBOX&MSG=2
GET /Session/9-CS6Tt1kjGCav2Hcz4ciY/Message.wssp?Mailbox=INBOX&MSG=3
GET /Session/9-CS6Tt1kjGCav2Hcz4ciY/Message.wssp?Mailbox=INBOX&MSG=4
GET /Session/9-CS6Tt1kjGCav2Hcz4ciY/Message.wssp?Mailbox=INBOX&MSG=5
No more more messages
10.0.0.105 - - [06/Feb/2007:16:26:22 GMT] "GET /xss.js HTTP/1.1" 200 41
http://127.0.0.1:8100/Session/9-
CS6Tt1kjGCav2Hcz4ciY/compose.wssp?OrigMessage=3&OrigMailbox=INBOX&Operation=Reply& -
> /xss.js
```

On successful exploitation of this vulnerability using the method above the attacker is left with a directory containing the contents of the user's inbox:-



The end result of this attack is a directory containing all email from the targeted user's inbox, however the attack is by no means limited to this and the vulnerability could be exploited to perform other attacks, for example, sending out spam from the user's account.

1.4. Recommendations

This section contains recommendations with respect to the CommuniGate application software. Included is a discussion of the specific vulnerability that was identified as well as best practice guidelines for the configuration of web application software. These recommendations were provided to the vendor when the issue was identified.

The vulnerability exists because the application fails to safely sanitise scripts embedded within emails. It is recommended that an additional layer of protection is added to HTML

encode all data that is returned back to the user as part of a layered security model that provides greater defence against attacks these kind of attacks.

This vulnerability is made simpler to exploit due to the way the application passes the session ID as a GET parameter. This is not in line with security best practice as within a shared PC environment this information may be cached and result in unauthorised access to the users account if the user has not correctly logged out of the application. Where a session ID is passed in a cookie this information is harder to obtain, although the document.cookie method may provide this access features like the HTTPOnly flag improve its security and a cookie value is not as easily obtainable as a referrer which is sent in most HTTP requests.

It is also recommended that where possible all users of the software be contacted and be advised to upgrade to the latest version once the issue has been resolved.

CommuniGate have taken steps to mitigate this vulnerability and the latest unaffected version can be obtained from the following locations:

== Valid Core License Keys: issued between 01-Oct-2004 and 31-Oct-2004, or on or after the 1st of Oct, 2005 ==

Solaris - Sparc

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-Solaris-Sparc-517.tar.gz>
<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-Solaris-Sparc-517.tar.gz>

Solaris - Intel

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-Solaris-Intel-517.tar.gz>
<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-Solaris-Intel-517.tar.gz>

MS Windows - Intel

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-Win32-Intel-517.zip>
<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-Win32-Intel-517.zip>

Linux (rpm-based) - Intel

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-Linux-5.1-7.i386.rpm>
<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-Linux-5.1-7.i386.rpm>

Linux (static and dynamic) - Intel

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-Linux-Intel-517.tgz>
<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-Linux-Intel-517.tgz>

Linux - x86_64

http://www.stalker.com/pub/CGatePro/5.1/CGatePro-Linux-5.1-7.x86_64.rpm
ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-Linux-5.1-7.x86_64.rpm

Linux - Itanium

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-Linux-5.1-7.ia64.rpm>
<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-Linux-5.1-7.ia64.rpm>

FreeBSD 4.x - Intel

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-FreeBSD4-Intel-517.tgz>
<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-FreeBSD4-Intel-517.tgz>

FreeBSD 5.x - Intel

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-FreeBSD5-Intel-517.tgz>

<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-FreeBSD5-Intel-517.tgz>

FreeBSD 6.x - Intel

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-FreeBSD5-Intel-517.tgz>

<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-FreeBSD5-Intel-517.tgz>

FreeBSD 5.x/6.x - x86_64

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-FreeBSD5-AMD64-517.tgz>

<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-FreeBSD5-AMD64-517.tgz>

MacOS X (Darwin) - PowerPC

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-Darwin-PPC-517.tgz>

<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-Darwin-PPC-517.tgz>

MacOS X (Darwin) - Intel

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-Darwin-Intel-517.tgz>

<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-Darwin-Intel-517.tgz>

HPUX - Itanium

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-HPUX-IA64-517.tar.gz>

<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-HPUX-IA64-517.tar.gz>

AIX - PPC

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-AIX-PPC-517.bff.Z>

<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-AIX-PPC-517.bff.Z>

NetBSD - Intel

<http://www.stalker.com/pub/CGatePro/5.1/CGatePro-NetBSD-Intel-517.tgz>

<ftp://ftp.stalker.com/pub/CGatePro/5.1/CGatePro-NetBSD-Intel-517.tgz>

MWR InfoSecurity
St. Clement House
1-3 Alencon Link
Basingstoke, RG21 7SB
Tel: +44 (0)1256 300920
Fax: +44 (0)1256 844083
mwrinfosecurity.com