[NEWS] Novell NetMail Multiple Vulnerabilities (Buffer Overflow and XSS)

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2005−09/0014.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 09/05/05

```
To: list@securiteam.com
Date: 5 Sep 2005 12:07:51 +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/mailinglist.html

− − − − − − − − −

Novell NetMail Multiple Vulnerabilities (Buffer Overflow and XSS)
−−−

```
00402CA2 lea ecx, [ebx+1] ; ebx is attacker controlled
00402CA5 push ecx
00402CA6 call MMmalloc
```

The MMalloc() routine performs minimal mathematical operations to the supplied value before allocating memory. An attacker can specify a malicious number that will result in an integer overflow and cause a small memory chunk to be allocated. The original and larger supplied value will be later used in an inline memcpy():

```
00402D6E rep movsd ; destination is attacker allocated
00402D70 mov ecx, edx
00402D72 and ecx, 3
00402D75 rep movsb
```

This instruction sequence will copy attacker−supplied data beyond the brims of the allocated heap chunk and arbitrarily overwrite the heap. Too large a payload will cause an access violation as it writes off the end of the heap. If the supplied data is large enough, it will corrupt the heap and eventually result in a classic arbitrary DWORD overwrite in NTDLL during subsequent heap manipulation:

```
77FCC2C0 mov [ecx], eax
77FCC2C2 mov [eax+4], ecx
```

By overwriting the address of a soon to be called function, the attacker can redirect CPU flow and eventually execute arbitrary code.

Successful exploitation of the described vulnerability allows unauthenticated remote attackers to execute arbitrary code with the privileges of the underlying user, normally NetMailService.

WebAccess Cross−Site Scripting:
When a user opens an appointment containing valid formatted script in the body of the message, the browser interprets and executes that script. The script could do perform malicious actions on the user's authenticated connection. This exploit is available to any client that sends an ical object to a NetMail user.

WebAccess Buffer Overflow:
Specifying a very large name on folder rename through the WebAccess or WebMail client causes a buffer Overflow that allow attackers to execute arbitrary code.

Vendor Status:
The vendor has issued a fix for the vulnerability:
<http://support.novell.com/filefinder/19357/index.html>
http://support.novell.com/filefinder/19357/index.html

CVE Information:
<http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1756>

CAN−2005−1756
<http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1757>
CAN−2005−1757
<http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1758>
CAN−2005−1758

Disclosure Timeline:
04/25/2005 − Initial vendor notification
04/25/2005 − Initial vendor response
09/01/2005 − Public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<mailto:idlabs−advisories@lists.idefense.com> iDEFENSE Labs Security
Advisories,
Novell.
The original article can be found at:
<http://www.idefense.com/application/poi/display?id=301&type=vulnerabilities>
http://www.idefense.com/application/poi/display?id=301&type=vulnerabilities
The vendor advisory can be found at:
<http://support.novell.com/cgi−bin/search/searchtid.cgi?/10097957.htm>
http://support.novell.com/cgi−bin/search/searchtid.cgi?/10097957.htm

==========

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.