

# [NEWS] Multiple Vulnerabilites in Nokia Intellisync Mobile Suite and Wireless Email Express

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00022.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 10 May 2007 16:05:21 +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>

-----

Multiple Vulnerabilites in Nokia Intellisync Mobile Suite and Wireless Email Express

---

## SUMMARY

<<http://europe.nokia.com/A4162029>> Nokia Intellisync Mobile Suite is "a portfolio of products that reside on a single server and can be used alone or together to create a comprehensive mobility solution. The Nokia Intellisync Mobile Suite server provides large businesses with the flexibility, manageability and extensibility to connect virtually any corporate data to virtually any device over almost any network to meet both current and future mobility needs". Multiple vulnerabilities have been found in Nokia's Intellisync Mobile Suite and Wireless Email Express, which allow remote attackers to gain access to sensitive information and cause denial of service.

Note: According to Nokia Austria support the tested versions were a bundle version from Novell to support Groupwise functionality hence Novell is responsible (according to Nokia).

It seems there exist many different versions of the same or very similar product. During a short review of an installation of Nokia Intellisync Wireless Email Express it was found to be partially vulnerable too.

## DETAILS

### Vulnerable Systems:

\* Nokia Intellisync Mobile Suite – Novell Groupwise bundle & Nokia Intellisync Wireless Email Express versions 6.4.31.2, 6.6.0.107, 6.6.2.2

### Vulnerability overview:

\* The bundled Apache Tomcat v5.0.25 suffers from an information disclosure vulnerability which allows an attacker to view the directory listing and the source code of the application.

\* Some ASP scripts under /usrmgr/ list all configured users including the mail server address with userid (but no password).

\* Furthermore it is possible to deactivate all users and denial access to the system.

\* Some ASP scripts are vulnerable to cross site scripting attacks.

An attacker does not need to be authenticated to perform those attacks!

### Vulnerability description:

1) Directory listing & source code information disclosure

It seems that (at least) versions v6.4.31.2, v6.6.0.107 and v6.6.2.2 are bundled with Apache Tomcat v5.0.25. This Tomcat version suffers from a known directory listing information disclosure vulnerability.

### Proof of concept:

Directory Listing: [http://\\$host/:jsp](http://$host/:jsp)

Source Code Disclosure: [http://\\$host/en/logon.asp;.jsp](http://$host/en/logon.asp;.jsp)

2) User accounts information disclosure

E.g., the following ASP scripts list all configured accounts:

/usrmgr/userList.asp

/usrmgr/userStatusList.asp

### Proof of concept:

userStatusList.asp outputs the following XML data for every account:

```
<f1>id</f1>
<f2>name</f2>
<f3>firstName</f3>
<f4>lastName</f4>
<f5>active</f5>
<f6>server</f6>
<f7>username</f7>
```

userList.asp additionally lists the configured timezone instead of the server address.

## [NEWS] Multiple Vulnerabilities in Nokia Intellisync Mobile Suite and Wireless Email Express

As the login name is known now an attacker can guess/brute force every account and check for weak passwords.

### 3) Unauthenticated user account deactivation denial of service

It is possible to deny access to the system for every user account. The script "userList.asp" also has the functionality to update the accounts. An unauthenticated attacker can change the login name, first name, last name and time zone settings. One can also change the "active" dropdown to "false" which deactivates the account.

By changing the login name to an empty value it is possible to hide the user. Only the id will show up in the overview page. One can still login with this username and the associated password.

Proof of concept:

The following URL shows the update page of the user with id 42:

[http://\\$host/usrmgr/userList.asp?action=update&userid=42](http://$host/usrmgr/userList.asp?action=update&userid=42)

### 4) Cross site scripting

It is possible to conduct cross site scripting attacks as input is not properly filtered in many scripts. Not all scripts were tested, hence it is likely that there are many more vulnerable scripts.

Proof of concept:

[http://\\$host/de/pda/dev\\_logon.asp?username=<script>alert\(42\)</script>&password=](http://$host/de/pda/dev_logon.asp?username=<script>alert(42)</script>&password=)

[http://\\$host/usrmgr/registerAccount.asp](http://$host/usrmgr/registerAccount.asp) (all fields)

[http://\\$host/de/create\\_account.asp](http://$host/de/create_account.asp)

[...]

Vendor contact timeline:

2007-03-19: vendor (Nokia/Intellisync) notified via email (mobile.business.emea@xxxxxxxxxx)

2007-03-20: no reply hence email to: sales@xxxxxxxxxxxxxxxxxx, software.marketing@xxxxxxxxxx, webmaster@xxxxxxxxxxxxxxxxxx

2007-03-20: sales replies and forwards to support@xxxxxxxxxxxxxxxxxx

2007-03-20: sending advisory draft to support@xxxxxxxxxxxxxxxxxx

2007-03-21: Nokia Austria support calls and needs more information (because they didn't get the advisory)

2007-03-23: Nokia Austria support says the product is a bundle version from Novell and they should be contacted

2007-03-23: contacted Novell regarding the issues (security@xxxxxxxxxx)

2007-03-27: Novell answered, SR # 10328518153 has been created

2007-03-28: SR updated, vulnerability should be handled by Nokia

2007-04-02: asking about the status again

2007-04-10: SR updated, "Nokia is looking into the issue"

2007-04-17: Nokia ticket has been opened, no word on it

2007-04-20: Nokia tested "GMS 2" where the issues are not reproduceable

Due to the lack of a "GMS 2" installation it couldn't be verified whether the issues have been resolved by Nokia. It is also unknown whether there's a newer version of Wireless Email Express that is not affected or whether

[NEWS] Multiple Vulnerabilites in Nokia Intellisync Mobile Suite and Wireless Email Express

there are more vulnerable Nokia products/versions.

Solution:

According to Nokia "GMS 2" is not affected, hence an upgrade is advised.

Workaround:

Restrict access to /usrmgr/ and manually upgrade Tomcat if possible.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:research@xxxxxxxxxxxxxxxx>>  
Johannes Greil.

The original article can be found at:

<<http://www.sec-consult.com/289.html>> <http://www.sec-consult.com/289.html>

=====

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@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====  
=====

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.