



**State of Alaska Cyber Security &
Critical Infrastructures
Cyber Advisory**

April 30, 2008

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

STATE OF ALASKA ADVISORY NUMBER:

2008-012

DATE(S) ISSUED:

April 30, 2008

SUBJECT:

Novell GroupWise Buffer Overflow Vulnerability

OVERVIEW:

A vulnerability in the Novell GroupWise System (Novell's Email system) has been identified. Successful exploitation of this vulnerability will allow an attacker to execute arbitrary code in the context of the application. This can result in an attacker gaining the same user privileges as the logged on user. If the user is logged in with administrator privileges, the attacker could then install programs, view, change, or delete data, or create new accounts with full privileges. This could lead to complete control of the compromised system.

SYSTEMS AFFECTED:

- Novell Groupwise 7.0.0
- Novell Groupwise 7.0.0 SP1
- Novell Groupwise 7.0.0 SP2
- Novell Groupwise 7.0.0 SP3
- Other versions may be affected

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

DESCRIPTION:

A new vulnerability in the Novell GroupWise System was discovered which affects the client-side application of Novell GroupWise. The application is prone to a buffer overflow vulnerability due to the in-adequate boundary checks on user supplied data. The end user only needs to view a malicious HTML formatted email or click on a specially crafted link designed to exploit this vulnerability. An attacker who successfully exploits an affected system could execute arbitrary code in the context of the application which can lead to complete control of the system. If the user is logged in with administrator privileges, the attacker could then install programs, view, change, or delete data, or create new accounts with full privileges. Failed attempts will result in a denial of service.

Currently there is proof-of-concept for the exploit available. Patches are not yet available.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Logon to your systems as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. Employ the principle of least privilege whenever possible.
- Do not open HTML formatted email, click on HTML links provided in an email, or open email attachments from an un-trusted source.

REFERENCES:

SecurityFocus:

<http://www.securityfocus.com/bid/28969>

FrSIRT:

<http://www.frsirt.com/english/advisories/2008/1393>