

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.*

**DATE(S) ISSUED:**

10/01/2012

**SUBJECT:**

Multiple Vulnerabilities in Novell GroupWise Could Allow Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Novell GroupWise which could allow remote code execution. Novell GroupWise is a collaborative software product, which includes email, calendars, instant messaging and document management. The GroupWise Internet Agent (GWIA) is a server component that provides communication to other email systems and conversion of email messages to GroupWise format.

Successful exploitation could allow an attacker to gain the same privileges as the affected application. An attacker could then install programs; view, change, or delete data; or create new accounts. Unsuccessful exploitation attempts may result in a denial of service.

**SYSTEMS AFFECTED:**

Versions prior to GroupWise 8.0 SP3

Versions prior to GroupWise 2012 Support Pack 1

**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:**

Multiple vulnerabilities have been discovered in GroupWise that can lead to remote code execution due to an unspecified error.

An integer overflow vulnerability has been discovered in GroupWise Internet Agent (GWIA) which could allow the attacker to execute arbitrary code on system with the privileges of the GroupWise application by causing a heap-based buffer overflow.

An unspecified vulnerability has been discovered in GroupWise Client which could allow the attacker to execute arbitrary code on the system with the privileges of the GroupWise application.

These vulnerabilities could be exploited via a specially crafted email or malicious website. In the email-based scenario, the user would have to open the specially crafted file as an email attachment. In the Web based scenario, a user would visit a website and then open the specially crafted file that is hosted on the page.

Successful exploitation could allow an attacker to gain the same privileges as the affected application. An attacker could then install programs; view, change, or delete data; or create new accounts. Unsuccessful exploitation attempts may result in a denial of service.

#### **RECOMMENDATIONS:**

The following actions should be taken:

For GroupWise 8 users, apply GroupWise 8.0 Support Pack 3 (or later) to vulnerable systems immediately after appropriate testing.

For GroupWise 2012 users, apply GroupWise 2012 Support Pack 1 to vulnerable systems immediately after appropriate testing.

Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

#### **REFERENCES:**

##### **Novell:**

<http://www.novell.com/support/kb/doc.php?id=7010770>

<http://www.novell.com/support/kb/doc.php?id=7010771>

##### **SecurityFocus:**

<http://www.securityfocus.com/bid/55729>

<http://www.securityfocus.com/bid/55731>

##### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0417>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0418>