

*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:**

02/01/2013

**SUBJECT:**

Multiple Vulnerabilities in Novell GroupWise Could Allow Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Novell GroupWise that could allow for remote code execution. Novell GroupWise is a collaborative software product that includes: email, calendars, instant messaging and document management.

Successful exploitation could allow an attacker to gain the same privileges as the affected user. 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:**

GroupWise Client for Windows 8.0x up to and including 8.0.3 HP1

GroupWise Client for Windows 2012 up to and including 2012.0 SP1

**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 untrusted pointer dereference errors.

An ActiveX Control vulnerability in GroupWise Client for Windows can be exploited by enticing a target user to open a malicious file or visit a malicious page, a remote attacker could execute arbitrary code on vulnerable installations of Novell GroupWise.

A vulnerability in GroupWise Client for Windows due to multiple untrusted pointer dereference vulnerabilities could be exploited by a remote attacker to compromise a vulnerable system.

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 user that could allow an attacker to make critical system modifications. 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 8.0.3 Hot Patch 2 (or later) to vulnerable systems immediately after appropriate testing.

For GroupWise 2012 users, apply GroupWise 2012 SP 1 Hot Patch 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=7011688>

<http://www.novell.com/support/kb/doc.php?id=7011687>

##### **SecurityFocus:**

<http://www.securityfocus.com/bid/57657>

<http://www.securityfocus.com/bid/57658>

##### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0439>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0804>