

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:

7/16/2010

SUBJECT:

Multiple Vulnerabilities in Novell GroupWise Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Novell GroupWise applications that could allow an attacker to take complete control of a vulnerable system. Novell GroupWise is a collaborative software product which includes email, calendars, instant messaging and document management. Successful exploitation of two of these vulnerabilities could result in an attacker gaining SYSTEM-level privileges on the affected system. The attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. The remaining vulnerabilities could allow for information disclosure. Failed exploit attempts may result in denial of service condition.

SYSTEMS AFFECTED:

- Novell Groupwise 6.5.0
- Novell Groupwise 6.5.0 SP1
- Novell Groupwise 7.0
- Novell Groupwise 7.0.0 SP1
- Novell Groupwise 7.0.0 SP2
- Novell Groupwise 7.0.0 SP3
- Novell Groupwise 7.0.0 SP4
- Novell Groupwise 7.01
- Novell Groupwise 7.02
- Novell Groupwise 7.03x
- Novell Groupwise 7.04
- Novell Groupwise 8.0
- Novell Groupwise 8.0 SP2
- Novell Groupwise 8.01x

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 Novell GroupWise applications that could allow an attacker to take complete control of a vulnerable system. Details of these vulnerabilities are as follows:

Novell GroupWise Internet Agent Stack Buffer Overflow Vulnerability

A stack-based buffer overflow vulnerability exists in the Novell GroupWise Internet Agent because it fails to perform adequate boundary checks on user-supplied data. Successful exploitation of this vulnerability could allow an attacker to gain SYSTEM-level privileges on the affected system. Failed exploit attempts may result in a denial-of-service condition.

Novell GroupWise Agents HTTP Interface HTTP Header Injection Vulnerability

The Novell GroupWise Agents HTTP Interface is prone to a HTTP Header Injection vulnerability which could allow an attacker to inject arbitrary HTTP headers resulting in redirecting users to malicious web links. This may lead to other attacks such as cross-site scripting, session hijacking, or cache poisoning.

Novell GroupWise Agents HTTP Interfaces Multiple Cross Site Scripting Vulnerabilities

The HTTP interfaces for Novell GroupWise agents are prone to multiple cross-site scripting vulnerabilities because it fails to sufficiently sanitize user-supplied input to the HTTP interfaces for Novell GroupWise agents. An attacker may leverage these vulnerabilities to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and launch other attacks.

Novell GroupWise WebAccess Proxy Feature Stack Buffer Overflow Vulnerability

The user Proxy feature of Novell GroupWise WebAccess is vulnerable to a stack-based buffer-overflow exploit. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code with SYSTEM-level privileges. Failed exploit attempts may result in a denial-of-service condition.

Novell GroupWise WebAccess HTML Injection Vulnerability

An HTML injection vulnerability has been identified in Novell GroupWise WebAccess. This vulnerability exists because the application fails to sufficiently sanitize user-supplied input before it is used in dynamically generated content. Successful exploitation of this vulnerability would allow for attacker supplied HTML and script code to run in the context of the affected Novell GroupWise WebAccess application, potentially allowing the attacker to steal cookie-based authentication credentials or to control how the site is rendered to the user.

Novell GroupWise WebAccess Cross-Site Scripting Vulnerabilities

Three cross-site scripting vulnerabilities exist in the Novell GroupWise WebAccess application. An attacker may leverage these vulnerabilities to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and launch other attacks.

Novell GroupWise WebAccess Authentication Information Disclosure Vulnerability

An information disclosure vulnerability exists in the way that Novell GroupWise WebAccess passes parameters to the affected web application. If successfully exploited, the attacker could gain access to authentication information in the user's web browser and this may lead to other attacks.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patch provided by Novell 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/viewContent.do?externalId=7006371>
<http://www.novell.com/support/viewContent.do?externalId=7006372>
<http://www.novell.com/support/viewContent.do?externalId=7006373>
<http://www.novell.com/support/viewContent.do?externalId=7006374>
<http://www.novell.com/support/viewContent.do?externalId=7006375>
<http://www.novell.com/support/viewContent.do?externalId=7006376>
<http://www.novell.com/support/viewContent.do?externalId=7006377>
<http://www.novell.com/support/viewContent.do?externalId=7006379>
<http://www.novell.com/support/viewContent.do?externalId=7006380>

Security Focus:

<http://www.securityfocus.com/bid/41704>
<http://www.securityfocus.com/bid/41705>
<http://www.securityfocus.com/bid/41706>
<http://www.securityfocus.com/bid/41707>
<http://www.securityfocus.com/bid/41710>
<http://www.securityfocus.com/bid/41711>
<http://www.securityfocus.com/bid/41712>
<http://www.securityfocus.com/bid/41713>
<http://www.securityfocus.com/bid/41714>

Secunia:

<http://secunia.com/advisories/40622>