

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

November 3, 2010

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.

ADVISORY NUMBER:
SA2010-084

DATE(S) ISSUED:
11/9/2010

SUBJECT:
Multiple Vulnerabilities in Novell GroupWise Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Novell GroupWise that could allow an attacker to take complete control of a vulnerable system. Novell GroupWise is a collaborative software product that includes email, calendars, instant messaging and document management. Successful exploitation of four 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 a denial of service condition.

SYSTEMS AFFECTED:

- Novell GroupWise 8.02

- Novell GroupWise 8.01x
- Novell GroupWise 8.0 SP2
- Novell GroupWise 8.0 SP1
- Novell GroupWise 8.0 HP2
- Novell GroupWise 8.0 HP1
- Novell GroupWise 8.0

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

Novell GroupWise Internet Agent (GWIA) IMAP Remote-Code Execution Vulnerabilities

Two vulnerabilities exist within the IMAP component of GWIA. One vulnerability occurs due to GWIA failing to handle the LIST command with a large parameter. The other vulnerability is caused by a specially crafted LIST or LSUB request. Successful exploitation of these vulnerabilities could result in remote-code execution.

Novell GroupWise Internet Agent (GWIA) 'Content-Type' Header Remote-Code Execution Vulnerabilities

Multiple vulnerabilities exist within 'gwia.exe' because it fails to properly parse multiple values, multiple string data and numbers within the 'Content-Type' header of received messages. Successful attacks could result in remote-code execution.

Novell GroupWise Internet Agent (GWIA) VCALENDAR Remote-Code Execution Vulnerabilities

Multiple vulnerabilities occur because the application fails to properly parse VCALENDAR messages. Three boundary errors exist within the 'gwww1.dll' when processing a RRULE, COMMENT or TZNAME variable which could allow for remote-code execution.

Novell GroupWise WebAccess Agent and Document Viewer Agent Input Validation Vulnerability

An input validation error exists in the WebAccess Agent and the Document Viewer Agent that could allow arbitrary files to be downloaded from the server. Successful exploitation would require authentication.

Novell GroupWise WebPublisher Cross-Site Scripting Vulnerability

WebPublisher is a component of GroupWise WebAccess that enables Web users to view GroupWise library documents that have been made public. This component is prone to a cross-site scripting vulnerability because it fails to properly sanitize unspecified input that gets passed to it. An attacker may leverage this vulnerability 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 Agents HTTP Interfaces Remote-Code Execution Vulnerabilities

An unspecified error exists in the HTTP interfaces for the Message Transfer Agent, Post Office Agent, Internet Agent, WebAccess Agent and Monitor agent which could allow for remote-code execution.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches 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=7007151>

<http://www.novell.com/support/viewContent.do?externalId=7007152>

<http://www.novell.com/support/viewContent.do?externalId=7007153>

<http://www.novell.com/support/viewContent.do?externalId=7007154>

<http://www.novell.com/support/viewContent.do?externalId=7007155>

Security Focus:

<http://www.securityfocus.com/bid/44732>

Zero Day Initiative:

<http://www.zerodayinitiative.com/advisories/ZDI-10-237>

<http://www.zerodayinitiative.com/advisories/ZDI-10-238>

<http://www.zerodayinitiative.com/advisories/ZDI-10-239>

<http://www.zerodayinitiative.com/advisories/ZDI-10-240>

<http://www.zerodayinitiative.com/advisories/ZDI-10-241>

<http://www.zerodayinitiative.com/advisories/ZDI-10-242>

<http://www.zerodayinitiative.com/advisories/ZDI-10-243>

Secunia:

<http://secunia.com/advisories/40820/>