

[NEWS] Gordano Messaging Suite – Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0045.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 09/16/03

To: list@securiteam.com

Date: 16 Sep 2003 15:36:05 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Gordano Messaging Suite – Multiple Vulnerabilities

SUMMARY

<<http://www.gordano.com>> Gordano Messaging Suite is "the powerful messaging server running on Windows, Linux, Solaris and AIX. It is being used by over twenty four thousand customers, in more than ninety countries, covering all sectors (Airlines, Press, Government Agencies, Education, Industry, etc)".

Multiple vulnerabilities in Gordano Messaging Suite (GMS) result in the ability to initiate a DoS attack and information disclosure (usernames, login time, domains, etc) attacks against the product.

DETAILS

Vulnerable systems:

* Gordano Messaging Suite version 9, build 3138

Remote DoS

The product's (WWW.exe the process) listens on the following ports to provide GMS Administration, WebMail Professional, WebMail Express, WebMail Mobile, Instant Messaging, and Web Server services to users: 80, 8000,

Securiteam: [NEWS] Gordano Messaging Suite – Multiple Vulnerabilities

8025, 8081, 8888, and 9000.

When a user sends a request like `../../../../` to GMS Web Server at port 80, the `WWW.exe` process will terminate, causing all the services that `WWW.exe` provides to shutdown immediately.

Example:

```
~$ telnet 192.168.1.69
Trying 192.168.1.69...
Connected to 192.168.1.69
Escape character is '^'.
GET ../../ HTTP/1.0
```

Connection closed by foreign host.

Under Linux, the vulnerability does not cause the `/gordano/bin/WWW` process to terminate. However, it never times out therefore if an attacker opens up like 15–20 connections (while sending `../../../../` requests), the process will be kept busy enough to deny any additional connections (from legitimate users).

Workaround:

Restarting the service is needed in order to gain normal functionality.

Information Disclosure [requires valid user credential]

`Alertlist.mml` provides information about users who have logged in to the GMS Server and discloses some useful information to the attackers such as usernames, domains, logged in time, etc. Moreover, it is supposed to be accessed by GMS Server's administrator only. However, a normal WebMail user is not denied access to it (<http://www.victim.com:8000/admin/reports/alertlist.mml>) allowing anyone to disclose this information.

Vendor status:

Vendor has verified the issues and has released a patch.

The patch can be downloaded by clicking on the following links:

* Linux platform:

ftp://ftp.gordano.com/gms/3138/hotfixes/h20030905/linux/www_h20030905.zip
ftp://ftp.gordano.com/gms/3138/hotfixes/h20030905/linux/www_h20030905.zip

* Windows platform:

ftp://ftp.gordano.com/gms/3138/hotfixes/h20030905/windows/www_h20030905.zip
ftp://ftp.gordano.com/gms/3138/hotfixes/h20030905/windows/www_h20030905.zip

ADDITIONAL INFORMATION

The information has been provided by <<mailto:dphuong@yahoo.com>> Phuong Nguyen.

=====

Securiteam: [NEWS] Gordano Messaging Suite – Multiple Vulnerabilities

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.