

# [VulnWatch] Digital Armaments: Apache auth\_ldap module Multiple Format Strings Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-01/msg00038.html>

---

- *From:* "Digital Armaments" <[vulnwatch@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:vulnwatch@xxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 30 Jan 2006 02:35:20 -0800 (PST)
- 

Apache auth\_ldap module Multiple Format Strings Vulnerability

<http://www.digitalarmaments.com/2006090173928420.html>

## I. Background

auth\_ldap is an LDAP authentication module for Apache, the world's most popular web server. auth\_ldap has excellent performance, and supports Apache on both Unix and Windows NT. It also has support for LDAP over SSL, and a mode that lets Microsoft Frontpage clients manage their web permissions while still using LDAP for authentication.

For further information or detail about the software you can refer to the vendor's homepage:

[http://www.rudedog.org/auth\\_ldap/](http://www.rudedog.org/auth_ldap/)

## II. Problem Description

Due to an insecure usage of the function apache logging function (ap\_log\_error) in auth\_ldap\_log\_reason function it's possible to run arbitrary code on the server running the module. For example this can generate a custom format string that can be supplied by the attacker through the username given during the apache authentication process but several parts of the module are affected.

## III. Detection

This problem has been detected on latest version of auth\_ldap 1.6.0 and on prior version from 1.2.x. It persists on all platforms where auth\_ldap can be compiled.

## IV. Impact analysis

Successful exploitation allows an attacker to gain access to the system. Exploit code is required.

## V. Solution

First notification 12.22.2005.

Second notification 01.09.2006.

The vendor answered second notification.

A new patched version is available.

## VI. Credit

Seregorin – seregorin@xxxxxxxxxxxxxx is credited with this discovery.

Get paid and get stocks by vulnerability submission

<http://www.digitalarmaments.com/contribute.html>

## VII. Legal Notices

Copyright © 2006 Digital Armaments LLC.

Redistribution of this alert electronically is allowed. It should not be edited in any way. Reprint the whole is allowed, partial reprint is not permitted. For any other request please email customerservice@xxxxxxxxxxxxxxxxxxxxxx for permission. Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

- 
- Prev by Date: [\*\[VulnWatch\] \[Argeniss\] Oracle Database Buffer overflows vulnerabilities in public procedures of XDB.DBMS XMLSCHEMA{ INT}\*](#)
  - Next by Date: [\*Re: \[VulnWatch\] Cisco Security Advisory: Cisco VPN 3000 Concentrator Vulnerable to Crafted HTTP Attack\*](#)
  - Previous by thread: [\*\[VulnWatch\] \[Argeniss\] Oracle Database Buffer overflows vulnerabilities in public procedures of XDB.DBMS XMLSCHEMA{ INT}\*](#)
  - Index(es):
    - ◆ [\*Date\*](#)
    - ◆ [\*Thread\*](#)