SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

Security Advisory Summary

The SolarWinds Information Security team has been made aware of CVE-2023-48795, a vulnerability concerning OpenSSH, an open source implementation of the SSH protocol, which enables attacker to downgrade authentication and effectively crack the password.

What happened?

A vulnerability was reported in the OpenSSH third party library. Exploiting SSH Terrapin allows a man-in-the-middle attacker to truncate important parts of the SSH handshake, without closing the SSH connection, which creates a security impact for the SSH client/server.

Advisory Details

Severity

5.9 Medium

Advisory ID

CVE-2023-48795

First Published

12/18/2023

Last Updated

1/29/2024

CVSS Score

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

Have there been any reports?

We have not received any reports from our customers of attacks related to this vulnerability.

How is SolarWinds addressing this?

For Security Event Manager (SEM), a fix is already in the works to prevent the issue from occurring and we recommend upgrading to the fix version once released.

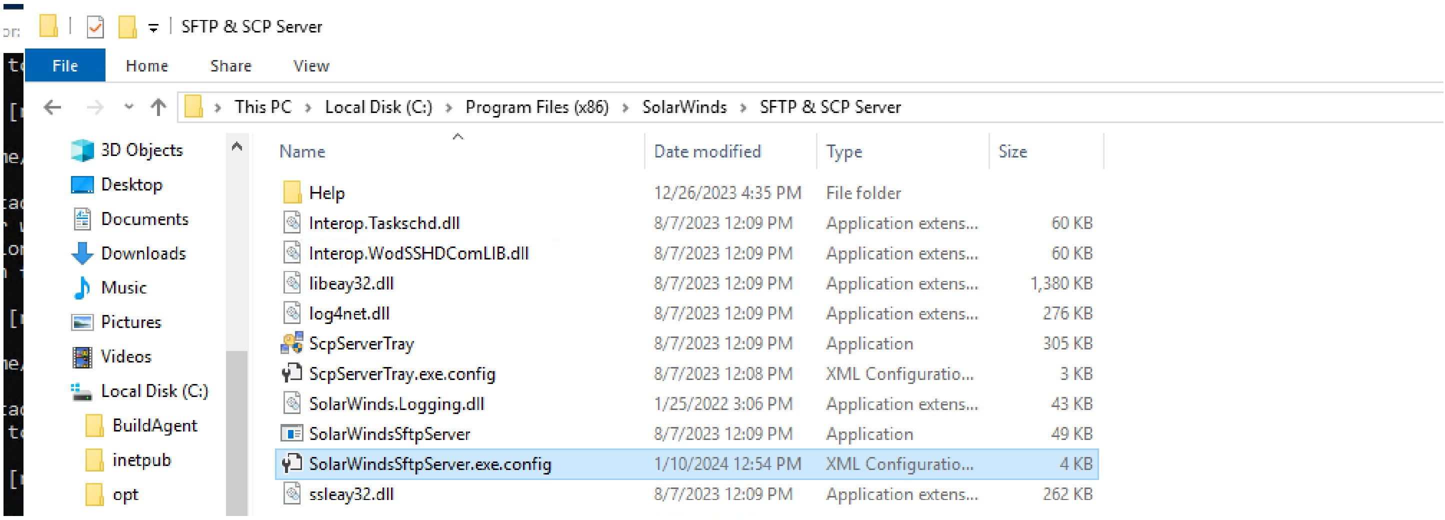
For SolarWinds SCP, a workaround will be provided to disable the vulnerable ChaCha20-Poly1305 cipher in the OpenSSH client and server configurations.

What actions should I take?

For Security Event Manager (SEM), a fix is already in the works to prevent the issue from occurring and we recommend upgrading to the fix version once released.

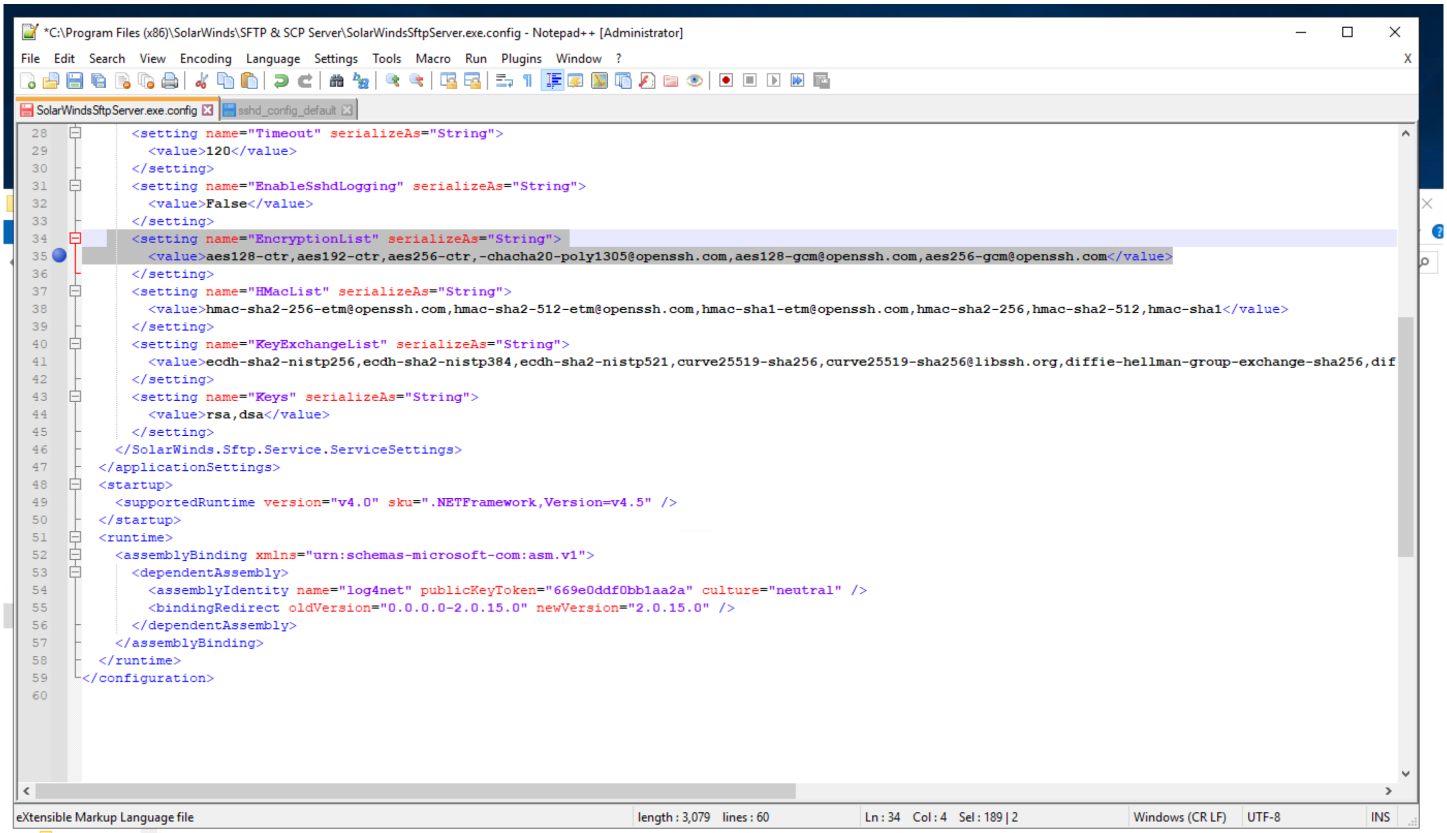
For SolarWinds SCP, Customers can follow the steps below to disable the vulnerable ChaCha20-Poly1305 cipher

- Go to this folder C:\Program Files (x86)\SolarWinds\SFTP & SCP Server and open the file SolarWindsSftpServer.exe.config with a text editor



Name	Date modified	Type	Size
Help	12/26/2023 4:35 PM	File folder	
Interop.Taskschd.dll	8/7/2023 12:09 PM	Application extens...	60 KB
Interop.WodSSHDComLIB.dll	8/7/2023 12:09 PM	Application extens...	60 KB
libeay32.dll	8/7/2023 12:09 PM	Application extens...	1,380 KB
log4net.dll	8/7/2023 12:09 PM	Application extens...	276 KB
ScpServerTray	8/7/2023 12:09 PM	Application	305 KB
ScpServerTray.exe.config	8/7/2023 12:08 PM	XML Configuratio...	3 KB
SolarWinds.Logging.dll	1/25/2022 3:06 PM	Application extens...	43 KB
SolarWindsSftpServer	8/7/2023 12:09 PM	Application	49 KB
SolarWindsSftpServer.exe.config	1/10/2024 12:54 PM	XML Configuratio...	4 KB
ssleay32.dll	8/7/2023 12:09 PM	Application extens...	262 KB

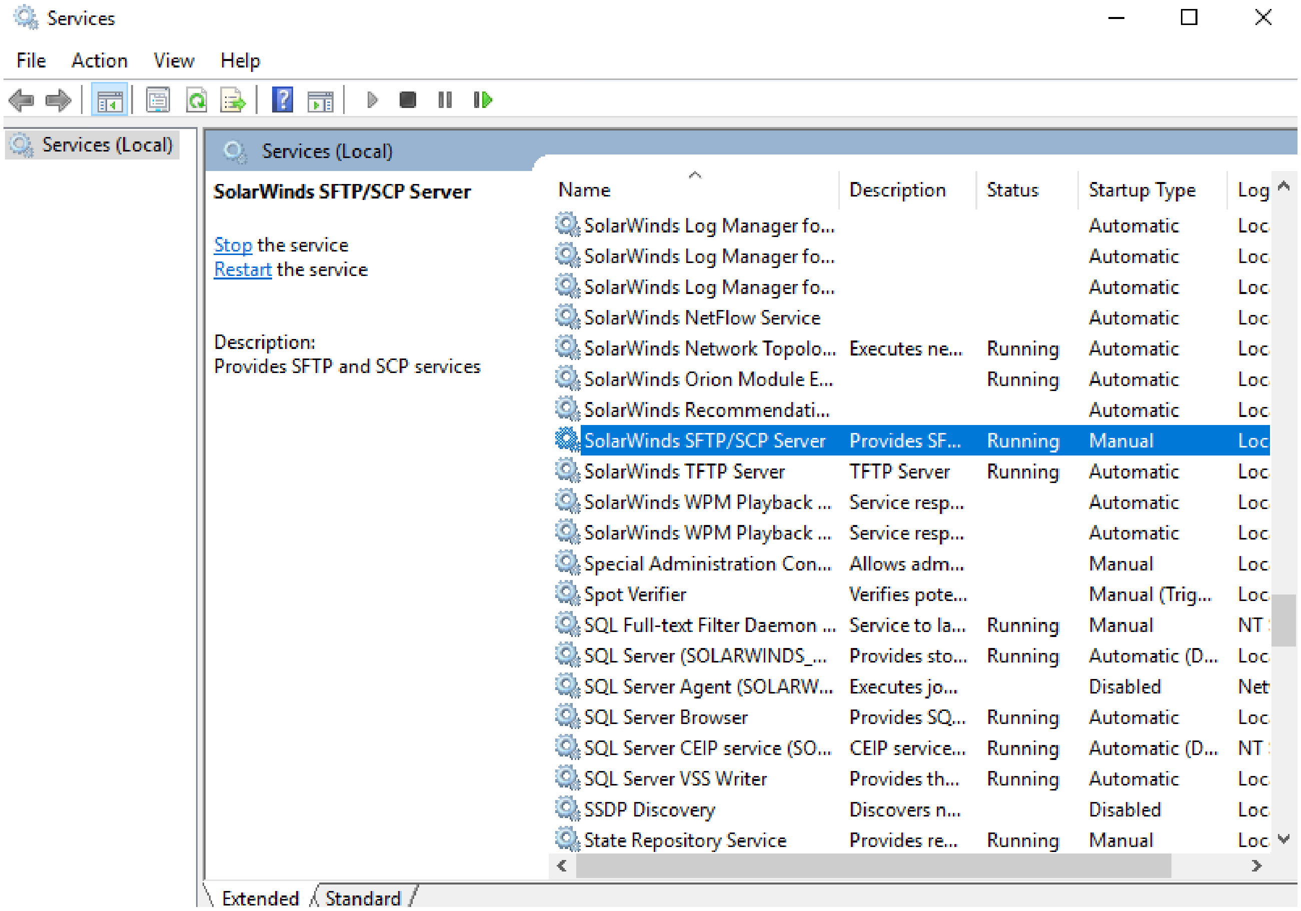
- Open the file with put a dash before the chacha20 in the highlighted line (Already done in this screenshot)


*C:\Program Files (x86)\SolarWinds\SFTP & SCP Server\SolarWindsSftpServer.exe.config - Notepad++ [Administrator]
File
Edit
Search
View
Encoding
Language
Settings
Tools
Macro
Run
Plugins
Window
?
SolarWindsSftpServer.exe.config
sshd_config_default

```
      <setting name="Timeout" serializeAs="String">
        <value>120</value>
      </setting>
      <setting name="EnableSshdLogging" serializeAs="String">
        <value>False</value>
      </setting>
      <setting name="EncryptionList" serializeAs="String">
        <value>aes128-ctr,aes192-ctr,aes256-ctr,-chacha20-poly1305@openssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com</value>
      </setting>
      <setting name="HMacList" serializeAs="String">
        <value>hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1</value>
      </setting>
      <setting name="KeyExchangeList" serializeAs="String">
        <value>ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group-exchange-sha256,dif
      </setting>
      <setting name="Keys" serializeAs="String">
        <value>rsa,dsa</value>
      </setting>
    </SolarWinds.Sftp.Service.ServiceSettings>
  </applicationSettings>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
  </startup>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="log4net" publicKeyToken="669e0ddf0bb1aa2a" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-2.0.15.0" newVersion="2.0.15.0" />
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
</configuration>
```

eXtensible Markup Language file
length : 3,079 lines : 60
Ln : 34 Col : 4 Sel : 189 | 2
Windows (CR LF)
UTF-8
INS

- Restart the Solarwinds SCP/SFTP Service



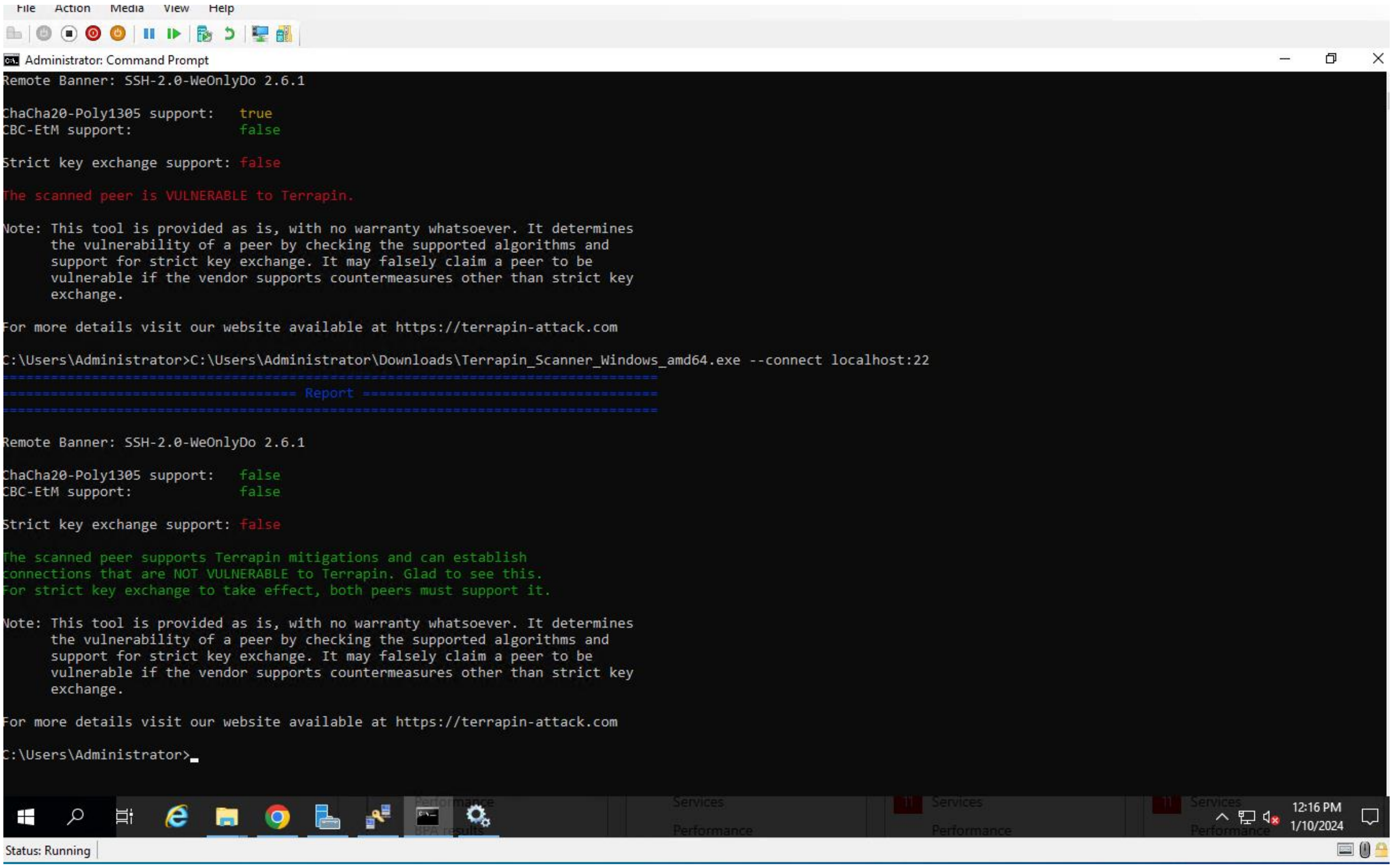
SolarWinds SFTP/SCP Server

Stop the service
Restart the service

Description:
Provides SFTP and SCP services

Name	Description	Status	Startup Type	Log
SolarWinds Log Manager fo...			Automatic	Loc
SolarWinds Log Manager fo...			Automatic	Loc
SolarWinds Log Manager fo...			Automatic	Loc
SolarWinds NetFlow Service			Automatic	Loc
SolarWinds Network Topolo...	Executes ne...	Running	Automatic	Loc
SolarWinds Orion Module E...		Running	Automatic	Loc
SolarWinds Recommendati...			Automatic	Loc
SolarWinds SFTP/SCP Server	Provides SF...	Running	Manual	Loc
SolarWinds TFTP Server	TFTP Server	Running	Automatic	Loc
SolarWinds WPM Playback ...	Service resp...		Automatic	Loc
SolarWinds WPM Playback ...	Service resp...		Automatic	Loc
Special Administration Con...	Allows adm...		Manual	Loc
Spot Verifier	Verifies pote...		Manual (Trig...	Loc
SQL Full-text Filter Daemon ...	Service to la...	Running	Manual	NT
SQL Server (SOLARWINDS_...	Provides sto...	Running	Automatic (D...	Loc
SQL Server Agent (SOLARW...	Executes jo...		Disabled	Net
SQL Server Browser	Provides SQ...	Running	Automatic	Loc
SQL Server CEIP service (SO...	CEIP service...	Running	Automatic (D...	NT
SQL Server VSS Writer	Provides th...	Running	Automatic	Loc
SSDP Discovery	Discovers n...		Disabled	Loc
State Repository Service	Provides re...	Running	Manual	Loc

- The top run of the scanner was before the above changes and the second run is after.



```
Remote Banner: SSH-2.0-WeOnlyDo 2.6.1

ChaCha20-Poly1305 support:   true
CBC-EtM support:             false

Strict key exchange support: false

The scanned peer is VULNERABLE to Terrapin.

Note: This tool is provided as is, with no warranty whatsoever. It determines
      the vulnerability of a peer by checking the supported algorithms and
      support for strict key exchange. It may falsely claim a peer to be
      vulnerable if the vendor supports countermeasures other than strict key
      exchange.

For more details visit our website available at https://terrapin-attack.com

C:\Users\Administrator>C:\Users\Administrator\Downloads\Terrapin_Scanner_Windows_amd64.exe --connect localhost:22
================================================================================
==================================== Report ====================================
================================================================================

Remote Banner: SSH-2.0-WeOnlyDo 2.6.1

ChaCha20-Poly1305 support:   false
CBC-EtM support:             false

Strict key exchange support: false

The scanned peer supports Terrapin mitigations and can establish
connections that are NOT VULNERABLE to Terrapin. Glad to see this.
For strict key exchange to take effect, both peers must support it.

Note: This tool is provided as is, with no warranty whatsoever. It determines
      the vulnerability of a peer by checking the supported algorithms and
      support for strict key exchange. It may falsely claim a peer to be
      vulnerable if the vendor supports countermeasures other than strict key
      exchange.

For more details visit our website available at https://terrapin-attack.com

C:\Users\Administrator>_
```

Affected Products

- SEM 2023.4 and previous versions
- Solarwinds SCP