



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Zeroday-Schwachstelle in SolarWinds Serv-U FTP Software ermöglicht Remote Code Execution (CVE-2021-35211)

CSW-Nr. 2021-234165-1032, Version 1.0, 13.07.2021

IT-Bedrohungslage*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Das US-Unternehmen SolarWinds stellt verschiedene Lösungen zur Netzwerk- und Systemadministration her. Zum Portfolio gehören auch die Produkte SolarWinds Serv-U Managed File Transfer Server und Serv-U Secured FTP, die einen sicheren Datentransfer inner- und außerhalb von Organisationen gewährleisten sollen.

Sicherheitsforscher des Microsoft Threat Intelligence Centers (MSTIC) und des Microsoft Offensive Security Research Teams haben in diesen Lösungen nun eine Zeroday-Schwachstelle CVE-2021-35211 [MIT2021] entdeckt, die einem Angreifer auf dem Zielsystem eine Remote Code Execution (RCE), die Installation von Programmen sowie die Manipulation und das Löschen von Daten ermöglicht [SOL2021a].

Betroffen sind alle Versionen bis einschließlich 15.2.3 HF1 und älter.

Nach den Angaben von SolarWinds soll die Schwachstelle jedoch nur dann ausnutzbar sein, wenn SSH in der SolarWind Serv-U Umgebung aktiviert ist.

- * 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Bewertung

Der Fall zeigt, dass neben der massiven Bedrohung durch Ransomware-Angriffe und deren unmittelbaren öffentlich sichtbaren Schädwirkungen – wie Ausfälle durch Neuaufsetzen von übernommen Netzen, Verschlüsselung der Daten und Abfluss und Veröffentlichung gestohlener Daten – eine latente Bedrohung durch Kompromittierung extern erreichbarer Systeme jederzeit besteht.

Maßnahmen

Das BSI empfiehlt, die durch den Hersteller zur Verfügung gestellten Sicherheitspatches zeitnah einzuspielen. Diese können über das Customer Portal von SolarWinds bezogen werden [SOL2021b].

Um weiterhin zu prüfen, ob Ihre SolarWinds Serv-U Umgebung kompromittiert worden ist, empfiehlt der Hersteller die Klärung der folgenden Fragen:

- **Haben Sie in Ihrer Serv-U Umgebung SSH aktiviert?**
Falls dies nicht der Fall ist, sind Sie von der beschriebenen Schwachstelle nicht betroffen. Die Installation des Patches sollte hiervon unabhängig in Betracht gezogen werden.
- **Haben Sie in Ihrer Umgebung ungewöhnliche Fehlermeldungen festgestellt?**
Beim vorliegenden Sachverhalt handelt es sich um eine sog. Return Oriented Programming (ROP) Attacke. Der Angreifer provoziert zunächst die Auslieferung einer Fehlermeldung, ehe er die Fehlerbehebungslogik des Programms ausnutzt, um eigene Befehle auszuführen. Bitte beachten Sie in diesem Zusammenhang, dass die bloße Ausgabe einer Fehlermeldung nicht zwingend mit einem Angriff zu tun haben muss.
- **Haben Sie die DebugSocketLog.txt gesichert?**
Speichern Sie die *DebugSocketlog.txt* Datei und überprüfen Sie, ob es in der Log-Datei zu den folgenden Fehlern gekommen ist:

```
07] Tue 01Jun21 02:42:58 - EXCEPTION: C0000005; CSUSSHSocket::ProcessReceive(); Type: 30; puchPayLoad = 0x041ec066; nPacketLength = 76; nBytesReceived = 80; nBytesUncompressed = 156; uchPaddingLength = 5
```

Andere Fehler können auch in diesem LogFile stehen, müssen aber nicht mit der Schwachstelle in Verbindung stehen.

- **Haben Sie evtl. auffällige Verbindungen via SSH beobachten können?**
Schauen Sie nach Verbindungen via SSH von den nachfolgend aufgelisteten IP-Adressen. Diese wurden als potentielle Angriffsindikatoren identifiziert:
 - › 98.176.196.89
 - › 68.235.178.32

Prüfen Sie auch die TCP Verbindungen des Ports 443 auf die IP-Adresse: 208.113.35.58

Des Weiteren empfiehlt das BSI den IT-Grundschutz APP.3.3: Fileserver (Edition 2021) im Umgang mit FTP-Servern zu beachten[BSI2021].

Links

[BSI2021] - IT-Grundschutz-Kompendium APP.3.3: Fileserver (Edition 2021)

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/06_APP_Anwendungen/APP_3_3_Fileserver_Edition_2021.pdf

[MIT2021] - MITRE zu CVE-2021-35211

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35211>

[SOL2021a] - SolarWinds Serv-U Remote Memory Escape Vulnerability Advisory

<https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211>

[SOL2021b] - SolarWinds Customer Portal Login
<https://customerportal.solarwinds.com/>

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

- 1) Was ist das Traffic Light Protokoll?
Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensiblen Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.
- 2) Welche Einstufungen existieren?
 - **TLP:WHITE: Unbegrenzte Weitergabe**
Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
 - **TLP:GREEN: Organisationsübergreifende Weitergabe**
Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
 - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
 - **TLP:RED: Persönlich, nur für benannte Empfänger**
Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.
- 3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
- 4) Was passiert, wenn ich die Einstufung nicht beachte?
Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.