Solutions ▼

Advisory Details

Products ▼

Serv-U Remote Memory Escape Vulnerability (CVE-2021-35211)

Trust Center Index Page > SolarWinds Trust Center Security Advisories | CVE-2021-35211

Security Vulnerability

Released: July 9, 2021

Last updated: July 15, 2021

Assigning CNA: SolarWinds

Security Advisory Summary

UPDATE July 15, 20201: You can Subscribe to this RSS Feed to be notified when we update this page (note: you will need to cut and paste the "Subscribe to this RSS feed" URL into an RSS Feed Reader, e.g., Outlook's RSS Subscriptions, to monitor updates). UPDATE July 13, 20201: We've provided additional indicators of compromise (IOCs) below. You can also

find additional details on the threat actor and their findings in a blog post from Microsoft.

Serv-U Secure FTP and does not affect any other SolarWinds or N-able (formerly SolarWinds MSP) products. SolarWinds was recently notified by Microsoft of a security vulnerability related to Serv-U Managed File <u>Transfer Server</u> and <u>Serv-U Secured FTP</u> and have developed a hotfix to resolve this vulnerability. While

UPDATE July 10, 2021: NOTE: This security vulnerability only affects Serv-U Managed File Transfer and

Microsoft's research indicates this vulnerability exploit involves a limited, targeted set of customers and a single threat actor, our joint teams have mobilized to address it quickly. The vulnerability exists in the latest Serv-U version 15.2.3 HF1 released May 5, 2021, and all prior versions. A threat actor who successfully exploited this vulnerability could run arbitrary code with

privileges. An attacker could then install programs; view, change, or delete data; or run programs on the affected system. Serv-U version 15.2.3 hotfix (HF) 2 has been released. Please see the **Security Updates** table below for the applicable update for your system. We recommend you install these updates immediately. If you are

unable to install these updates, see the FAQ in this Security Advisory for information on how to help protect your system from this vulnerability.

for the protection of their environments. **Affected Products** Serv-U 15.2.3 HF1 and all prior Serv-U versions

Additional details of the vulnerability will be published after giving customers sufficient time to upgrade

Fixed Software Release Serv-U 15.2.3 HF2

Security Updates

Software Version

Serv-U 15.2.3 HF1

Serv-U 15.2.3	Apply Serv-U 15.2.3 HF1, then apply Serv-U 15.2.3 HF2, available in your Customer Portal
All Serv-U versions prior to 15.2.3	Upgrade to Serv-U 15.2.3, then apply Serv-U 15.2.3 HF1, then apply Serv-U 15.2.3 HF2, available in your Customer Portal
Acknowledgements	
SolarWinds would like to thank the Security Resemanner and working with our security, product, a	earcher below for reporting on the issue in a responsible and engineering teams to fix the vulnerability.
Microsoft Threat Intelligence Center (MSTIC) ar	

Upgrade Paths

Customer Portal

Apply Serv-U 15.2.3 HF2, available in your

Description

Disclaimer

Please note, any content posted herein is provided as a suggestion or recommendation to you for your internal use. This is not part of the SolarWinds software or documentation that you purchased from SolarWinds, and the information set forth herein may come from third parties. Your organization should

internally review and assess to what extent, if any, such custom scripts or recommendations will be incorporated into your environment. You elect to use third-party content at your own risk, and you will be

Revision Date

solely responsible for the incorporation of the same if any.

Revisions

Version

Updated FAQ information. Added July 15, 2021 RSS feed instructions. These are 1.4 informational changes only. Updated FAQ information. This is July 13, 2021 1.3 an informational change only. Updated FAQ information. This is 1.2 July 10, 2021 an informational change only. Notice added, updated FAQ July 10, 2021 information. This an 1.1 informational change only. 1.0 July 9, 2021 Information Published

actor may be able to gain privileged access to the threat actor on the machine hosting Serv-U.

FAQ

Have SolarWinds customers been affected? Microsoft has provided evidence of limited, targeted customer impact, though SolarWinds does not

What happened?

Have N-able customers been affected? No, N-able customer who do not use Serv-U are not affected by this vulnerability. Updated July 13, 2021

currently have an estimate of how many customers may be directly affected by the vulnerability.

product. The Linux versions of these products **are not vulnerable** to a RCE exploit of this security vulnerability. The Linux version of the Serv-U product crashes when the exploit is attempted by a threat actor.

SolarWinds is unaware of the identity of the potentially affected customers.

All other SolarWinds and N-able (formerly SolarWinds MSP) are not affected by this vulnerability. This

Updated July 15, 2021

What products are not affected?

What products are affected?

includes the Orion Platform, and all Orion Platform modules. A complete list of products not known to be affected by this security vulnerability follows: SolarWinds product NOT AFFECTED by this security vulnerability: 8Man

 Application Centric Monitor (ACM) Network Topology Mapper (NTM) AppOptics

 Papertrail Backup Document

Patch Manager

Network Operations Manager (NOM)

Network Performance Monitor (NPM)

Access Rights Manager (ARM)

 Backup Profiler Pingdom Backup Server

 Pingdom Server Monitor Backup Workstation Server & Application Monitor (SAM)

 CatTools Server Configuration Monitor (SCM) Dameware Mini Remote Control

Security Event Manager (SEM)

 Dameware Patch Manager Security Event Manager Workstation Edition Dameware Remote Everywhere

 Service Desk Dameware Remote Manager Server Profiler

 Database Performance Analyzer (DPA) Storage Manager Database Performance Analyzer Integration Module*(DPAIM*)

 Storage Profiler Database Performance Monitor (DPM) Storage Resource Monitor (SRM)

 DNSstuff Threat Monitor

 Engineer's Toolset Virtualization Manager (VMAN) Engineer's Web Toolset

Virtualization Profiler

Firewall Security Monitor

High Availability (HA)

BI Sentry

 Enterprise Operations Console (EOC) VoIP & Network Quality Manager (VNQM) FailOverEngine Web Help Desk

 SQL Sentry Identity Monitor DB Sentry IP Address Manager (IPAM)

Web Performance Monitor (WPM)

 V Sentry ipMonitor Win Sentry KiwiCatTools

 Kiwi Log Viewer SentryOneDocument Kiwi Syslog Server SentryOneTest LANSurveyor

 Task Factory Librato DBAxPress Log Analyzer (LA)

 Plan Explorer Log & Event Manager (LEM) APS Sentry Log & Event Manager Workstation Edition

 Mobile Admin SentryOneMonitor NetFlow Traffic Analyzer (NTA) BlxPress

SQL Sentry Essentials

DW Sentry

Loggly

Network Automation Manager (NAM)

 Patch Backup Disaster Recovery Automation Manager M365 Backup

Updated July 13, 2021 How can I tell if my environment has been compromised? The following steps are steps you can take to determine if your environment has been compromised:

does not exist.

C:\ProgramFiles\RhinoSoft\Serv-U\DebugSocketlog.txt In the log file **DebugSocketlog.txt** you may see an exception, such as:

C:\ProgramData\RhinoSoft\Serv-U\DebugSocketlog.txt

U Assistance" and our team will assist you (no login required).

thrown, so an exception itself is not necessarily an indicator of attack.

nBytesUncompressed = 156; uchPaddingLength = 5 Exceptions may be thrown for other reasons so please collect the logs to assist with determining your situation.

3. Are you seeing potentially suspicious connections via SSH? Look for connections via SSH from the following IP addresses, which have been reported as a potential indicator of attack by the threat actor:

hxxp://144[.]34[.]179[.]162/a C:\Windows\Temp\Serv-u.bat C:\Windows\Temp\test\current.dmp

platforms for Serv-U.exe spawning anomalous processes, such as:

 .\Client\Common type [a file path] > "C:\ProgramData\RhinoSoft\Serv-U\Users\Global Users\[file name].Archive" Any process with the following in the command line:

Global users information. Serv-U Management Console - Server

This list shows the global user accordonains. If you observe this activity, investigate these processes further, and any traffic originating from the Serv-U

What kind of vulnerability is this?

Based on our investigations, this is a remote code execution (RCE) exploit. What versions of Serv-U are affected?

Updated July 13, 2021 Where can I get additional information? We understand the desire for more information on this issue, and we'll provide more information here as

it's available.

©2024 SolarWinds Worldwide, LLC. All rights reserved.

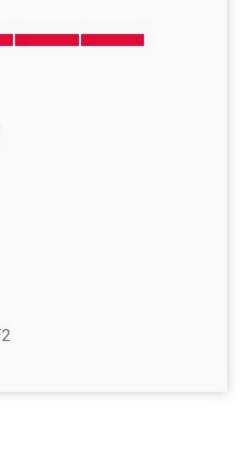
We're Geekbuilt.®

SOLARWINDS

The result? IT management products that are effective, accessible, and easy to

Career Center Preference Center **Trust Center GDPR Resource Center** Secure by Design Security Information

Company



Severity 9.0 Critical Advisory ID CVE-2021-35211 First Published 07/09/2021 **Last Updated** 07/15/2021 **Fixed Version** Serv-U 15.2.3 HF2

Resources •

Quote →

Microsoft reported to SolarWinds that they had discovered a remote code execution (RCE) vulnerability in the SolarWinds Serv-U product. Microsoft provided a proof of concept of the exploit. If exploited, a threat To the best of our understanding, no other SolarWinds products have been affected by this vulnerability. Only SolarWinds Serv-U Managed File Transfer and Serv-U Secure FTP for Windows are affected by this vulnerability. Please note the Serv-U Gateway is a component of these two products and is not a separate

 Network Configuration Manager (NCM) *NOTE: Please note DPAIM is an integration module and is not the same as Database Performance Analyzer (DPA). We have also found no evidence that any of our free tools, (TFTP/SCP), Orion agents, or Web Performance Monitor (PM) Players are impacted by this security vulnerability. N-able (formerly SolarWinds MSP) products NOT AFFECTED by this security vulnerability: N-central – Probe Mail Assure N-central – Topology SpamExperts N-central –NetPath MSP Manager N-central PassPortal NetPath – Server Take Control RMM Webprotection Backup How is SolarWinds addressing this? SolarWinds released a hotfix Friday, July 9, 2021, and we recommend all customers using Serv-U install this fix immediately for the protection of your environment. Updated July 10, 2021 What actions should I take? If you are an active maintenance SolarWinds customer of the Serv-U product, SolarWinds asks you to log into your Customer Portal to access your updates. This update is expected to take only a few minutes to implement. If you are not on active maintenance and currently using a Serv-U product, our Customer Success team

is available to help you with your questions. Please open a customer service ticket with the subject "Serv-

1. Is SSH enabled for your Serv-U installation? If SSH is not enabled in the environment, the vulnerability

2. Is your environment throwing exceptions? This attack is a Return Oriented Programming (ROP) attack. When exploited, the vulnerability causes the Serv-U product to throw an exception and then intercepts the

exception handling code to run commands. Please note, several reasons exist for exceptions to be

Please collect the **DebugSocketlog.txt** log file, which can be found in the following locations:

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

98[.]176[.]196[.]89

68[.]235[.]178[.]32

208[.]113[.]35[.]58

144[.]34[.]179[.]162

mshta.exe

powershell.exe

97[.]77[.]97[.]58 Other indicators:

4. Are you seeing potentially suspicious activity by Serv-U? Review your monitoring tools and/or EDR

The addition of any unrecognized Global users to Serv-U. This can be checked in the users tab of

 cmd.exe (or conhost.exe then spawning cmd.exe) with any of the following in the command line: whoami dir ./Client/Common

the Serv-U Management Console, as shown below. It can also be checked by looking for recently created files in C:\ProgramData\RhinoSoft\Serv-U\Users\Global Users, which appears to store the

C:\Windows\Temp\

Serv-U Management Console Dashboard & Users - Create, modify, and delete glob Global Users Database Users

investigation. Is this vulnerability related to the SUNBURST cyberattack? No. It's important to note this new vulnerability is completely unrelated to the SUNBURST supply chain attack. Software vulnerabilities are quite common, range in severity levels, and are routinely resolved by

box. Please contact SolarWinds Customer Support with this information, and we will escalate for

Based on our investigations, this RCE exploit affects all versions of Serv-U, prior to version 15.2.3 HF2, which has been built to address this vulnerability, and to help protect your environment.

software vendors as part of their ongoing maintenance release schedules.

In the meantime, our Customer Success team is available to you. Please open a <u>customer service ticket</u> with the subject "Serv-U Assistance" and our team will assist you (no login required).

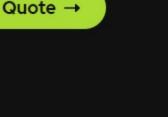
Developed by network and systems engineers who know what it takes to manage today's dynamic IT environments, SolarWinds has a deep connection to the IT

For Customers For Community Documentation **Resource Center**

IT Glossary

For Government

Investors



f 💆 🖸 in