From: **Anthony Paiz** apaiz@runbeck.net
Subject: Re: MS-ISAC CYBERSECURITY ADVISORY - A Vulnerability in TeamViewer Cloud Allow for Offline Password Cracking - PATCH: NOW - TLP: WHITE
Date: August 24, 2020 at 8:15 AM
To: Lynch, Britni Britni.Lynch@co.snohomish.wa.us, Fell, Garth Garth.Fell@co.snohomish.wa.us
Cc: Jonathan Wright jwright@runbeck.net, Harris, Randy /o=ExchangeLabs/ou=Exchange Administrative Group /cn=Recipients/cn=e91bc8239193484bb88efa073c3064b4-Harris, Ran>, Braathen, JD /o=ExchangeLabs/ou=Exchange Administrative Group /cn=Recipients/cn=a19366b1a146437189b06c863b453bac-Braathen, J>, Joseph Ferrara jferrara@runbeck.net

CAUTION : This email originated from outside of this organization. Please exercise caution with links and attachments.

Thanks Britni

ANTHONY PAIZ
Vice President, Field Services

RUNBECK ELECTION SERVICES Inc.
BEST WORKPLACE in the AMERICAS 2020
VoteCORE™ Election Management System

a: 2800 S. 36th Street, Phoenix, AZ 85034
d: 480-455-1013 I **c:** 602-550-3159
runbeck.net

From: "Lynch, Britni" <Britni.Lynch@co.snohomish.wa.us>
Date: Monday, August 24, 2020 at 8:02 AM
To: Anthony Paiz <apaiz@runbeck.net>, "Fell, Garth" <Garth.Fell@co.snohomish.wa.us>
Cc: Jonathan Wright <jwright@runbeck.net>, "Harris, Randy" <Randall.Harris@co.snohomish.wa.us>, "Braathen, JD" <Jon.Braathen@co.snohomish.wa.us>, Joseph Ferrara <jferrara@runbeck.net>
Subject: Re: MS-ISAC CYBERSECURITY ADVISORY - A Vulnerability in TeamViewer Cloud Allow for Offline Password Cracking - PATCH: NOW - TLP: WHITE

Good morning,

Joe can reach out to me at anytime to coordinate this update.

Thank you,

Britni Lynch

Elections Inbound Ballot Specialist

Snohomish County Auditor's Office

3000 Rockefeller Avenue, M/S 505

Everett, WA 98201-4059

425-262-2285 | britni.lynch@snoco.org | www.snoco.org

Notice: All emails and attachments sent to and from Snohomish County are public records and may be subject to disclosure pursuant to the Public Records Act (RCW 42.56).

From: Anthony Paiz <apaiz@runbeck.net>
Sent: Monday, August 24, 2020 7:20 AM
To: Fell, Garth <Garth.Fell@co.snohomish.wa.us>
Cc: Jonathan Wright <jwright@runbeck.net>; Lynch, Britni <Britni.Lynch@co.snohomish.wa.us>; Harris, Randy <Randall.Harris@co.snohomish.wa.us>; Braathen, JD <Jon.Braathen@co.snohomish.wa.us>; Joseph Ferrara <jferrara@runbeck.net>
Subject: Re: MS-ISAC CYBERSECURITY ADVISORY - A Vulnerability in TeamViewer Cloud Allow for Offline Password Cracking - PATCH: NOW - TLP: WHITE

CAUTION : This email originated from outside of this organization. Please exercise caution with links and attachments.

Good Morning Garth,

Not sure if my email went through last night but wanted to follow up.

We have received an updated TeamViewer version that complies with the identified vulnerability. The team will need to remote in and update the version. I can have Joe Ferrara reach out to your team at their convenience to upgrade both units.

Take care,

ANTHONY PAIZ
Vice President, Field Services

RUNBECK ELECTION SERVICES Inc.
BEST WORKPLACE in the AMERICAS 2020
VoteCORE™ Election Management System

a: 2800 S. 36th Street, Phoenix, AZ 85034
d: 480-455-1013 l **c:** 602-550-3159
runbeck.net

From: "Fell, Garth" <Garth.Fell@co.snohomish.wa.us>

From: Fell, Garth <Garth.Fell@co.snohomish.wa.us>
Date: Sunday, August 23, 2020 at 1:31 PM
To: Anthony Paiz <apaiz@runbeck.net>
Cc: Jonathan Wright <jwright@runbeck.net>, "Lynch, Britni" <Britni.Lynch@co.snohomish.wa.us>, "Harris, Randy" <Randall.Harris@co.snohomish.wa.us>, "Braathen, JD" <Jon.Braathen@co.snohomish.wa.us>, Joseph Ferrara <jferrara@runbeck.net>
Subject: RE: MS-ISAC CYBERSECURITY ADVISORY - A Vulnerability in TeamViewer Cloud Allow for Offline Password Cracking - PATCH: NOW - TLP: WHITE

Anthony,

Did I miss an update on TeamViewer and whether there is anything we need to do?

Garth Fell
County Auditor

Snohomish County Auditor's Office
3000 Rockefeller Avenue
Everett, WA 98201
425-388-3472 | garth.fell@snoco.org | www.snoco.org

Notice: All emails and attachments sent to and from Snohomish County are public records and may be subject to disclosure pursuant to the Public Records Act (RCW 42.56).

From: Anthony Paiz [mailto:apaiz@runbeck.net]
Sent: Wednesday, August 5, 2020 2:43 PM
To: Fell, Garth <Garth.Fell@co.snohomish.wa.us>
Cc: Jonathan Wright <jwright@runbeck.net>; Lynch, Britni <Britni.Lynch@co.snohomish.wa.us>; Harris, Randy <Randall.Harris@co.snohomish.wa.us>; Braathen, JD <Jon.Braathen@co.snohomish.wa.us>; Joseph Ferrara <jferrara@runbeck.net>
Subject: RE: MS-ISAC CYBERSECURITY ADVISORY - A Vulnerability in TeamViewer Cloud Allow for Offline Password Cracking - PATCH: NOW - TLP: WHITE

Good Afternoon Garth,

Thank you for sending this to me. We received this alert as well this morning. I'm currently working with TeamViewer now to identify vulnerabilities and if there are patches associated with our version. We currently utilize TV 9.0.224135. I will follow up with more detail as soon as I have something to share.

Hope you had a successful election yesterday.

Take care,

ANTHONY PAIZ
Vice President, Field Services

a: 2800 S. 36th Street, Phoenix, AZ 85034
d: 480-455-1013 l **c:** 602-550-3159
runbeck.net

From: Fell, Garth <Garth.Fell@co.snohomish.wa.us>
Sent: Wednesday, August 5, 2020 10:36 AM
To: Anthony Paiz <apaiz@runbeck.net>
Cc: Lynch, Britni <Britni.Lynch@co.snohomish.wa.us>; Harris, Randy <Randall.Harris@co.snohomish.wa.us>; Braathen, JD <Jon.Braathen@co.snohomish.wa.us>
Subject: FW: MS-ISAC CYBERSECURITY ADVISORY - A Vulnerability in TeamViewer Cloud Allow for Offline Password Cracking - PATCH: NOW - TLP: WHITE
Importance: High

Anthony,

Does this advisory apply to the version of TeamViewer deployed with Agilis environment? What is your recommendation in regards to any action that may need to take place?

Thanks,

Garth Fell
Snohomish County Auditor

Sent from my Verizon, Samsung Galaxy smartphone

-------- Original message --------

Original message

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Date: 8/5/20 7:28 AM (GMT-08:00)
To: Michael Aliperti <Michael.Aliperti@cisecurity.org>
Subject: MS-ISAC CYBERSECURITY ADVISORY - A Vulnerability in TeamViewer Cloud Allow for Offline Password Cracking - PATCH: NOW - TLP: WHITE

CAUTION : This email originated from outside of this organization. Please exercise caution with links and attachments.

TLP: WHITE

MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2020-106

DATE(S) ISSUED:
08/05/2020

SUBJECT:
A Vulnerability in TeamViewer Cloud Allow for Offline Password Cracking

OVERVIEW:
A vulnerability has been discovered in TeamViewer, which could allow for offline password cracking. TeamViewer is a program used for remote control, desktop sharing, online meetings, web conferencing, and file transfer between systems. Successful exploitation of this vulnerability could allow an attacker to launch TeamViewer with arbitrary parameters. The program could be forced to relay an NTLM authentication request to the attacker's system allowing for offline rainbow table attacks and brute force cracking attempts. These attacks could lead to further exploitation due to stolen credentials from successful exploitation of this vulnerability.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

1. TeamViewer versions 15.8.3 and prior

RISK:
Government:

1. Large and medium government entities: **High**
2. Small government entities: **Medium**

Businesses:

1. Large and medium business entities: **High**
2. Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in TeamViewer, which could allow for offline password cracking. Specifically, this vulnerability is due to the program not properly quoting its custom URI handlers. This vulnerability can be exploited when the system

visits a maliciously crafted website.

Successful exploitation of this vulnerability could allow an attacker to launch TeamViewer with arbitrary parameters. The program could be forced to relay an NTLM authentication request to the attacker’s system allowing for offline rainbow table attacks and brute force cracking attempts. These attacks could lead to further exploitation due to stolen credentials from successful exploitation of this vulnerability.

RECOMMENDATIONS:
We recommend the following actions be taken:

3. Apply appropriate patches from TeamViewer to the vulnerable systems after appropriate testing.
4. Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
5. Inform and educate users regarding threats posed by hypertext links contained in emails or attachments, especially from un-trusted sources.

REFERENCES:
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13699

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
https://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .

"This e-mail message (and any attachment) is intended for the use of the individual or entity to which it is addressed. This message contains information from Runbeck Election Services, Inc. that may be privileged, confidential, or exempt from disclosure under applicable law. If you are not the intended recipient or authorized to receive this for the intended recipient, any use, dissemination, distribution, retention, archiving, or copying of this communication is strictly prohibited. If you have received this e-mail in error, please notify the sender immediately by reply e-mail, delete this message, and delete the material from all computers."

"This e-mail message (and any attachment) is intended for the use of the individual or entity to which it is addressed. This message contains information from Runbeck Election Services, Inc. that may be privileged, confidential, or exempt from disclosure under applicable law. If you are not the intended recipient or authorized to receive this for the intended recipient, any use, dissemination, distribution, retention, archiving, or copying of this communication is strictly prohibited. If you have received this e-mail in error, please notify the sender immediately by reply e-mail, delete this message, and delete the material from all computers."

"This e-mail message (and any attachment) is intended for the use of the individual or entity to which it is addressed. This message contains information from Runbeck Election Services, Inc. that may be privileged, confidential, or exempt from disclosure under applicable law. If you are not the intended recipient or authorized to receive this for the intended recipient, any use, dissemination, distribution, retention, archiving, or copying of this communication is strictly prohibited. If you have received this e-mail in error, please notify the sender immediately by reply e-mail, delete this message, and delete the material from all computers."