Post de Kevin Beaumont

Kevin Beaumont
Cyber weatherman
3 mois · Modifié

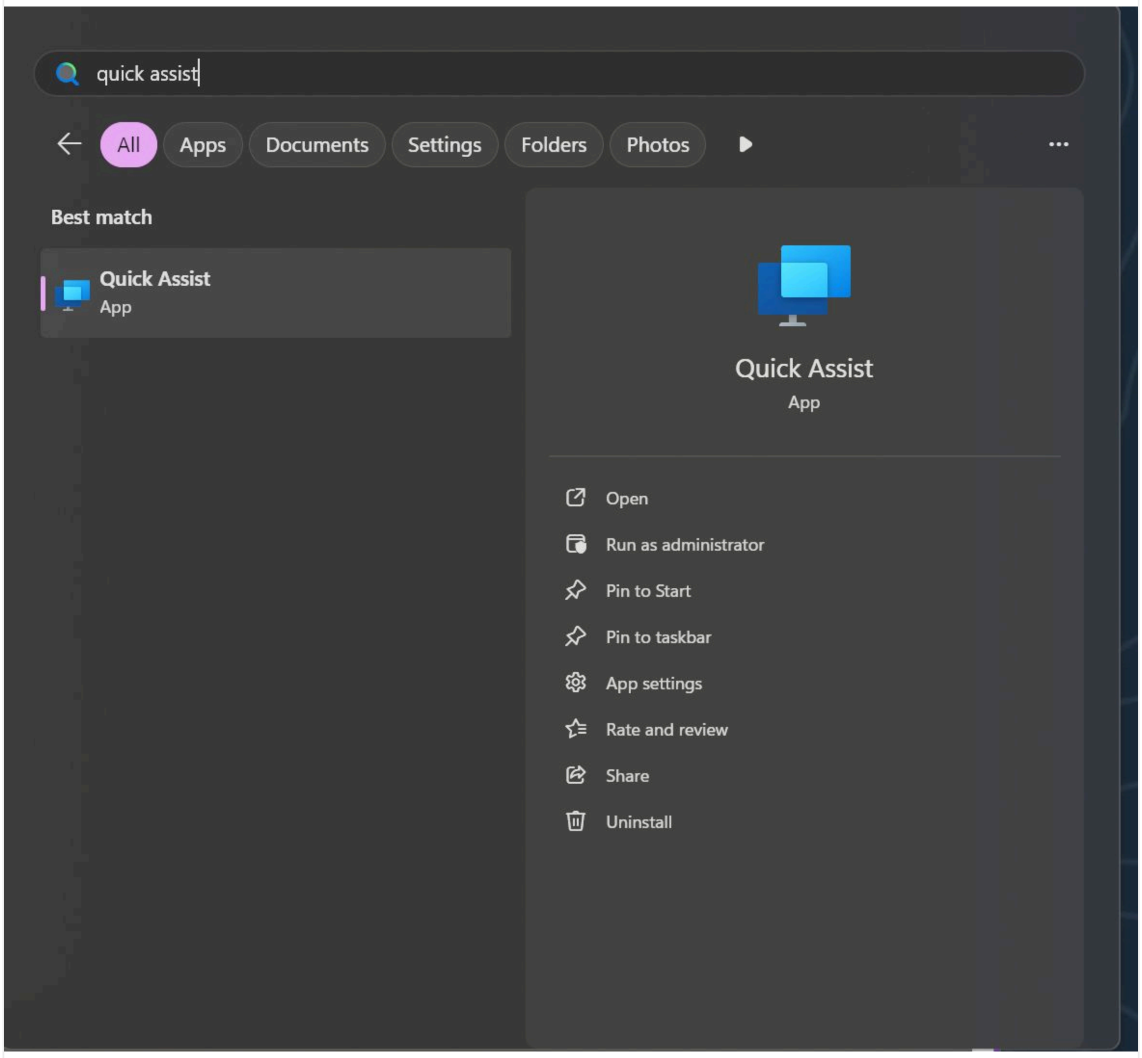
I've been assisting a few orgs hit with successful ransomware deployment lately where two newish things are at play - sharing is caring. They're doing initial recon over the phone for contact details, then flooding the users with email and/or Teams spam (think thousands of messages an hour).

Then they phone up and pretend to be from IT to stop the spam - they use Microsoft Quick Assist to take remote control of the system, and install an SSH reverse shell backdoor, and stop the spam run. From there they hand off to another team, who move laterally and get domain admin, then another team does exfiltration and another encrypts.

Two key learnings:

- Get users to report very high volumes of spam to local IT support, and not accept blind calls to help - verify somehow.

- Microsoft Quick Assist is installed *by default* in Windows 10 and 11, including in the Professional and Enterprise SKUs, and traverses firewalls and VPNs by design. To check your system, Windows key - type Quick and look for Quick Assist. All it takes to connect for a remote attacker is a 6 digit PIN. Remove the feature centrally, it's a big loophole.



1 695 · 111 commentaires

J'aime · Commenter · Partager

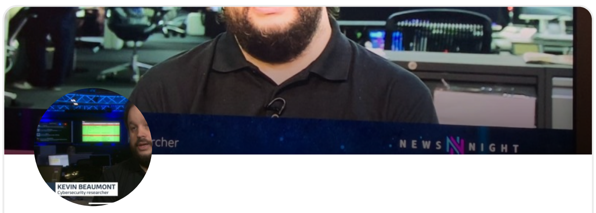
Atharv Nikude · 3 mois
Security Researcher | Cyber Security Enthusiast | Network & Web Security | Penetration Tester | VA...

If attackers are exploiting default tools like Microsoft Quick Assist so effectively, should organizations rethink allowing pre-installed remote support software altogether ?

J'aime · Réagir | 3 réactions

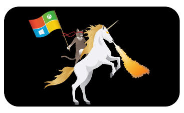
Adam Heathcote · 3 mois
Senior Systems Administrator at University of Tasmania

Or suggest an endpoint protection mechanism that would detect an SSH reverse shell and kill the process. There is almost no legitimate reason to run one in a



15 226 abonnés
443 posts · 1 article
Voir le profil · + Suivre

Publié par le même auteur



Detection tips for users of Defender Endpoint
Kevin Beaumont · 4 ans

Explorer les sujets

Vente
Marketing
Services informatiques
Administration des affaires
Gestion des ressources humaines
Ingénierie
Compétences générales
Tout voir

Windows centric environment. If your Windows endpoints are starting reverse SSH sessions they should be isolated automatically.

J'aime · Réagir | 12 réactions

Ts. Muhammad Haris Jafri 3 mois ···
Google Cloud Certified Digital Leader | Azure Security Engineer Associate | Microsoft Security Ope...

Is it Black Basta Ransomware?

https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/

J'aime · Réagir | 1 réaction

Richard Roy 3 mois
IT Manager Versaterm USA

Quick assist does not allow admin access. They would need to make then end user do the install.
Beyond that inbound ssh is blocked by default to all systems and av is on by default.
I don't think the details you are peoviding are complete.

J'aime · Réagir | 2 réactions

John Courtenay 3 mois
New role starting 17th March 2025

I didn't even know this existed, must be a newer version of what used to be Remote Assistance, definitely worth making sure this is disabled via GPO on corporate networks!

J'aime · Réagir | 1 réaction

Abraham Raher 3 mois
Technical Writer / graphista / renewables advocate / ex-Criblanian

Thanks for this, Kevin Beaumont!

Typo:

From there they had off to another team

should read

From there they hand off to another team

J'aime · Réagir | 1 réaction

Dominique (Dom) Côté 3 mois
SoloPro: Business Class IT zum Economy Preis - speziell für GründerInnen und KMU. #MSFTFanBoi

Do NOT remove quick assist, unless you have another remote support tool in place that is independent of Windows or M365!

This is so misleading again... 🤦

This is not a Quick Assist problem.
It applies to Teams, Zoom, Slack and any other tool that allows unidentified / unauthenticated external contacts.

Which is the whole point of modern work - easy collaboration with everyone.

Educating users is the solution here! Teach them to get confirmation from their own it first or generally never accept support from outside the company. Teach them how to positively id internal it support before granting screen access.

Quick Assist is an invaluable tool and as an MSP I can say it is our last resort access to customers pcs in emergencies.

That being said: we tell our customers to only use Teams to contact us and we use Teams for screen sharing. Thats positive ID, backed by Entra phishing resistant MFA.

J'aime · Réagir | 35 réactions

Dominika Jadowska 3 mois
Senior Technical Support Expert

Not to hate on the post.

But. If Quick Assist is a security issue it's the same issue with any software allowing remote control.

If a bad actor is lucky enough for an org to use Zoom, Teams, Google Meets (Put any enterprise software that's common enough and has remote desktop features) this can be exploited.

Quick Assist is a nice last line of assistance for a remote employee :/

The higher importance should be placed in educating people to not trust a "Microsoft" tech calling you blindly and trying to help with your device that has no issues...

If you can't trust your employees you either employ the wrong people or don't provide adequite training.

J'aime · Réagir | 5 réactions

Izabella STUEFLOTTEN, MBA 3 mois
Cyber Risk & GRC strategist @ Elasticito | GRC Ambassador of the Year Award 2024 | Cybersecurit...

Several biases are also at play here! If we can educate our workforce about being aware of these, that would be helpful in avoiding attacks.

1) Authority bias: they trust "IT" and so comply with their requests to give remote control.

2) Urgency bias: they make poor decisions when they are stressed (by being flooded with spam) and want it solved so they can get on with their work.

I wrote an article just yesterday about some other types of biases you should be aware of.

J'aime · Réagir | 6 réactions

Russell Gower-Leech 3 mois
Cyber Security Manager at Select Technology Systems Ltd

Presumably the victims had local admin permissions if the threat actors were able to install SSH?

Another basic tip - 99% of the time users do not need admin rights

J'aime · Réagir | 2 réactions

Voir plus de commentaires

Identifiez-vous pour afficher ou ajouter un commentaire

Plus de posts pertinents

Joe V.
Cybersecurity Professional, Dad, Husband, and Advice-Giver
3 mois

We've been seeing the same attack pretext launched against several clients in the past few months. Thankfully has not led all the way through to ransomware, but the initial denial of service and phony IT hero call is identical here. Be wary folks, and know your support process.

Whether it's internal IT or an external MSP, know the expected path to getting them to help - I promise they will not be magically reaching out over Teams if you haven't called them already. And I double promise that they should already have a means of accessing your machine remotely, none of which will require you granting them a code or any other set of credentials. When in doubt, call them back on a known-good line.

Kevin Beaumont
Cyber weatherman
3 mois · Modifié

I've been assisting a few orgs hit with successful ransomware deployment lately where two newish things are at play - sharing is caring. They're doing initial recon over the phone for contact details, then flooding the users with email and/or Teams spam (think thousands of messages an hour).

Then they phone up and pretend to be from IT to stop the spam - they use Microsoft Quick Assist to take remote control of the system, and install an SSH reverse shell backdoor, and stop the spam run. From there they hand off to another team, who move laterally and get domain admin, then another team does exfiltration and another encrypts.

Two key learnings:

- Get users to report very high volumes of spam to local IT support, and not accept blind calls to help - verify somehow.

- Microsoft Quick Assist is installed *by default* in Windows 10 and 11, including in the Professional and Enterprise SKUs, and traverses firewalls and VPNs by design. To check your system, Windows key - type Quick and look for Quick Assist. All it takes to connect for a remote attacker is a 6 digit PIN. Remove the feature centrally, it's a big loophole.

8 · 1 commentaire

J’aime   Commenter   Partager

Identifiez-vous pour afficher ou ajouter un commentaire

Tristan Watkins
Microsoft technology generalist, with deep specialism in Identity, Security + Compliance. Wi...
3 mois

Interesting new ransomware fatigue tactics seen in the wild. This is similar to the MFA prompt fatigue tactics that have been well-known (and very successful) for a while. If your users are inundated with huge volumes of SPAM, they need to be educated not to accept inbound calls (and definitely not remote assistance following an inbound call) to help with that.

Kevin Beaumont
Cyber weatherman
3 mois · Modifié

I've been assisting a few orgs hit with successful ransomware deployment lately where two newish things are at play - sharing is caring. They're doing initial recon over the phone for contact details, then flooding the users with email and/or Teams spam (think thousands of messages an hour).

Then they phone up and pretend to be from IT to stop the spam - they use Microsoft Quick Assist to take remote control of the system, and install an SSH reverse shell backdoor, and stop the spam run. From there they hand off to another team, who move laterally and get domain admin, then another team does exfiltration and another encrypts.

Two key learnings:

- Get users to report very high volumes of spam to local IT support, and not accept blind calls to help - verify somehow.

- Microsoft Quick Assist is installed *by default* in Windows 10 and 11, including in the Professional and Enterprise SKUs, and traverses firewalls and VPNs by design. To check your system, Windows key - type Quick and look for Quick Assist. All it takes to connect for a remote attacker is a 6 digit PIN. Remove the feature centrally, it's a big loophole.

J'aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire

Ricardo Flores Cedillo
Infraestructura en redes digitales | Ciberseguridad | Hacking Etico | CCTV | SOC Analyst
2 mois

I've been assisting a few orgs hit with successful ransomware deployment lately where two newish things are at play - sharing is caring. They're doing initial recon over the phone for contact details, then flooding the users with email and/or Teams spam (think thousands of messages an hour).

Then they phone up and pretend to be from IT to stop the spam - they use Microsoft Quick Assist to take remote control of the system, and install an SSH reverse shell backdoor, and stop the spam run. From there they hand off to another team, who move laterally and get domain admin, then another team does exfiltration and another encrypts.

Two key learnings:

- Get users to report very high volumes of spam to local IT support, and not accept blind calls to help - verify somehow.

- Microsoft Quick Assist is installed *by default* in Windows 10 and 11, including in the Professional and Enterprise SKUs, and traverses firewalls and VPNs by design. To check your system, Windows key - type Quick and look for Quick Assist. All it takes to connect for a remote attacker is a 6 digit PIN. Remove the feature centrally, it's a big loophole.

2

J'aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire

Ashiq Shaikh
IT Support Technician @ Lakeside Performance Gas Services Ltd.
3 mois · Modifié

Here's a great example that highlights the necessity of user training to prevent social engineering attacks 🛡️. The weakest link in an organization's cybersecurity posture always traces back to - the people, the end users 🧑 💻. #phishing #vishing #socialengineering

The #quickassist application on Windows 10/11 does not allow the remote user to perform administrator-level actions. Because of this, the attacker's first step was to install an SSH reverse-shell backdoor — which was then used to move laterally and get domain admin privileges.

Kevin Beaumont
Cyber weatherman
3 mois · Modifié

I've been assisting a few orgs hit with successful ransomware deployment lately where two newish things are at play - sharing is caring.   They're doing initial recon over the phone for contact details, then flooding the users with email and/or Teams spam (think thousands of messages an hour).

Then they phone up and pretend to be from IT to stop the spam - they use Microsoft Quick Assist to take remote control of the system, and install an SSH reverse shell backdoor, and stop the spam run. From there they hand off to another team, who move laterally and get domain admin, then another team does exfiltration and another encrypts.

Two key learnings:

- Get users to report very high volumes of spam to local IT support, and not accept blind calls to help - verify somehow.

- Microsoft Quick Assist is installed *by default* in Windows 10 and 11, including in the Professional and Enterprise SKUs, and traverses firewalls and VPNs by design. To check your system, Windows key - type Quick and look for Quick Assist. All it takes to connect for a remote attacker is a 6 digit PIN. Remove the feature centrally, it's a big loophole.

2

J’aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire

Peter Strate
Senior Security Consultant @ Syndis | Cybersecurity, Security operations, Sales Growth
3 mois

REMOVE MICROSOFT QUICK ASSIST FROM YOUR USERS COMPUTERS!

This post addresses a problem you should handle quickly - with Black Friday and all the upcoming holidays here and phishing attempts are skyrocketing the least you should do is to turn of Microsoft Quick Assist on all computers!

Kevin Beaumont
Cyber weatherman
3 mois · Modifié

I've been assisting a few orgs hit with successful ransomware deployment lately where two newish things are at play - sharing is caring. They're doing initial recon over the phone for contact details, then flooding the users with email and/or Teams spam (think thousands of messages an hour).

Then they phone up and pretend to be from IT to stop the spam - they use Microsoft Quick Assist to take remote control of the system, and install an SSH reverse shell backdoor, and stop the spam run. From there they hand off to another team, who move laterally and get domain admin, then another team does exfiltration and another encrypts.

Two key learnings:

- Get users to report very high volumes of spam to local IT support, and not accept blind calls to help - verify somehow.

- Microsoft Quick Assist is installed *by default* in Windows 10 and 11, including in the Professional and Enterprise SKUs, and traverses firewalls and VPNs by design. To check your system, Windows key - type Quick and look for Quick Assist. All it takes to connect for a remote attacker is a 6 digit PIN. Remove the feature centrally, it's a big loophole.

4

J’aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire

Oren Elimelech
Cyber Security & Privacy Researcher & Adviser | Speaker | Accedmy Lecturer | Global Chief In…
3 mois

1st, thank you for the important insights.
2nd, As a CISO, I see the increasing threat of social engineering attacks as a critical issue. Raising user awareness is essential, as these attacks exploit human psychology to gain unauthorized access. Training programs, especially those using gamification, can effectively engage employees and improve their ability to recognize and respond to these threats.Moreover, it’s vital to regularly audit endpoints for remote support software like Microsoft Quick Assist, TeamViewer, SplashTop, Anydesk, AmmyAdmin and similars, look for new installations and even block/monitor such traffic.Be alert for RMM tools such as Ninja, Atera, ConnectWise and others. These can be exploited if not properly secured, making them potential entry points for attackers. By combining user education with stringent endpoint checks, we can significantly bolster our cybersecurity defenses.
Remember, Security should beBuilt-in not Bolt-on.

#CISO #Cybersecurity #infosec #CyberTeam360

Kevin Beaumont
Cyber weatherman
3 mois · Modifié

I've been assisting a few orgs hit with successful ransomware deployment lately where two newish things are at play - sharing is caring. They're doing initial recon over the phone for contact details, then flooding the users with email and/or Teams spam (think thousands of messages an hour).

Then they phone up and pretend to be from IT to stop the spam - they use Microsoft Quick Assist to take remote control of the system, and install an SSH reverse shell backdoor, and stop the spam run. From there they hand off to another team, who move laterally and get domain admin, then another team does exfiltration and another encrypts.

Two key learnings:

- Get users to report very high volumes of spam to local IT support, and not accept blind calls to help - verify somehow.

- Microsoft Quick Assist is installed *by default* in Windows 10 and 11, including in the Professional and Enterprise SKUs, and traverses firewalls and VPNs by design. To check your system, Windows key - type Quick and look for Quick Assist. All it takes to connect for a remote attacker is a 6 digit PIN. Remove the feature centrally, it's a big loophole.

12

J’aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire

Graham Thomson
Chief Information Security Officer | Cyber Security Consultant | Security Strategy Adviser | Te…
3 mois

Great advice from Kevin, and worth checking in your business if Quick Assist is enabled.

Kevin Beaumont
Cyber weatherman
3 mois · Modifié

I've been assisting a few orgs hit with successful ransomware deployment lately where two newish things are at play - sharing is caring. They're doing initial recon over the phone for contact details, then flooding the users with email and/or Teams spam (think thousands of messages an hour).

Then they phone up and pretend to be from IT to stop the spam - they use Microsoft Quick Assist to take remote control of the system, and install an SSH reverse shell backdoor, and stop the spam run. From there they hand off to another team, who move laterally and get domain admin, then another team does exfiltration and another encrypts.

Two key learnings:

- Get users to report very high volumes of spam to local IT support, and not accept blind calls to help - verify somehow.

- Microsoft Quick Assist is installed *by default* in Windows 10 and 11, including in the Professional and Enterprise SKUs, and traverses firewalls and VPNs by design. To check your system, Windows key - type Quick and look for Quick Assist. All it takes to connect for a remote attacker is a 6 digit PIN. Remove the feature centrally, it's a big loophole.

3

J'aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire

Brian S.
Network/System Security Architect | CISSP
3 mois

A couple take aways... Kill Quick Assist and make sure your clients know what the "official" channel(s) is(are) for communication with internal IT/support. #buildawareness

Kevin Beaumont
Cyber weatherman
3 mois · Modifié

I've been assisting a few orgs hit with successful ransomware deployment lately where two newish things are at play - sharing is caring. They're doing initial recon over the phone for contact details, then flooding the users with email and/or Teams spam (think thousands of messages an hour).

Then they phone up and pretend to be from IT to stop the spam - they use Microsoft Quick Assist to take remote control of the system, and install an SSH reverse shell backdoor, and stop the spam run. From there they hand off to another team, who move laterally and get domain admin, then another team does exfiltration and another encrypts.

Two key learnings:

- Get users to report very high volumes of spam to local IT support, and not accept blind calls to help - verify somehow.

- Microsoft Quick Assist is installed *by default* in Windows 10 and 11, including in the Professional and Enterprise SKUs, and traverses firewalls and VPNs by design. To check your system, Windows key - type Quick and look for Quick Assist. All it takes to connect for a remote attacker is a 6 digit PIN. Remove the feature centrally, it's a big loophole.

1

J’aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire

Wei Ren T.
GCFA, EnCE, CCME, and MCFE certified. Working on enhancing my skills in IR.
3 mois

Reminder that the tools available in your system are PLENTY for threat actors to perform their malicious actions.

Everybody should be aware of the most common security risks such as:
1) Remote Desktop
2) Powershell

Kevin Beaumont
Cyber weatherman
3 mois · Modifié

I've been assisting a few orgs hit with successful ransomware deployment lately where two newish things are at play - sharing is caring. They're doing initial recon over the phone for contact details, then flooding the users with email and/or Teams spam (think thousands of messages an hour).

Then they phone up and pretend to be from IT to stop the spam - they use Microsoft Quick Assist to take remote control of the system, and install an SSH reverse shell backdoor, and stop the spam run. From there they hand off to another team, who move laterally and get domain admin, then another team does exfiltration and another encrypts.

Two key learnings:

- Get users to report very high volumes of spam to local IT support, and not accept blind calls to help - verify somehow.

- Microsoft Quick Assist is installed *by default* in Windows 10 and 11, including in the Professional and Enterprise SKUs, and traverses firewalls and VPNs by design. To check your system, Windows key - type Quick and look for Quick Assist. All it takes to connect for a remote attacker is a 6 digit PIN. Remove the feature centrally, it's a big loophole.

9

J’aime Commenter Partager

Identifiez-vous pour afficher ou ajouter un commentaire