

NAS da QNAP

Manual de Segurança da Informação
- NAS da QNAP



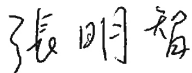
QNAP SYSTEMS, INC.

As melhores práticas para melhorar a segurança

Obrigado por utilizar os produtos QNAP e por confiar os seus dados ao NAS da QNAP para o armazenamento em segurança. Agradecemos muito o seu apoio e consideramos a sua confiança em nós como o nosso bem mais precioso. Para tal, procuramos a perfeição, melhorando constantemente os nossos produtos e a segurança.

No mundo de hoje, com um número crescente de ataques, malware e preocupações de segurança, sentimos a necessidade de disponibilizarmos as seguintes informações para o ajudar a defender-se de forma proativa e a proteger os seus ativos digitais. Esperamos que, ao combinar o aconselhamento prestado neste guia com hábitos sensatos de utilização das TI, todos os nossos utilizadores possam proteger os seus dispositivos e dados contra ameaças atuais e emergentes.

QNAP Systems, Inc.



Diretor-Geral

www.qnap.com

Os métodos de proteção de dados estão constantemente a tentar acompanhar a evolução das técnicas de hacking (acesso ilícito - pirataria informática). Para manter os seus dados e dispositivos protegidos, os utilizadores do NAS têm muitas ferramentas à sua disposição - incluindo proteção por palavra-passe, definições de permissão, encriptação ao nível de ficheiros, atualizações do sistema operativo e software, definições de ligação de rede e aplicações para cópia de segurança de dados e recuperação de desastres. Os produtos da QNAP têm características de segurança da informação multifacetadas e robustas. Abaixo encontram-se nove (9) pontos de segurança da informação para ajudar os nossos utilizadores a obterem rapidamente uma compreensão básica da segurança da informação.

1. Remover contas de utilizador desconhecidas ou suspeitas
2. Remover aplicações NAS desconhecidas ou raramente utilizadas
3. Desativar definições automáticas do router no myQNAPcloud
4. Configurar os controlos de acesso ao dispositivo
5. Não divulgar o número da porta predefinida na Internet
6. Instalar e executar a última versão do Malware Remover
7. Alterar de forma recorrente as palavras-passe de cada conta de utilizador
8. Atualizar as aplicações instaladas para as versões mais recentes
9. Garantir que o sistema operativo e/ou o software do sistema dos seus dispositivos em rede estão sempre atualizados

Mais tarde, explicaremos, um a um, os vários projetos de segurança da informação da QNAP e iremos elaborar um plano de defesa abrangente do NAS.

Usar palavras-passe fortes

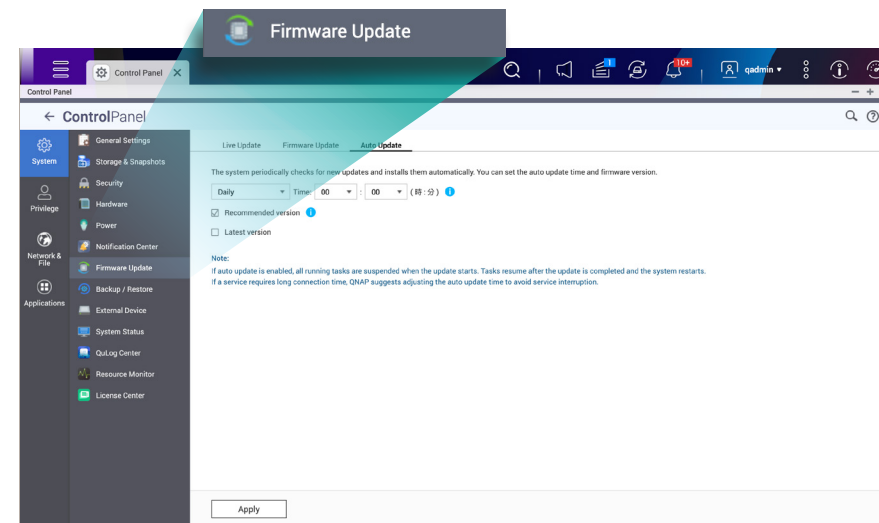
A tentativa de aceder à conta de um utilizador é o vetor de ataque mais comum para os hackers (piratas informáticos). Isto é normalmente realizado por hackers que tentam palavras-passe comuns ou predefinidas ou utilizando engenharia social (por exemplo, se alguém usou o nome de um animal de estimação ou de uma criança como palavra-passe, alguém pode ser capaz de a adivinhar). Para atenuar a ameaça de uma conta de utilizador ser comprometida, recomendamos a desativação da conta de administrador predefinida e a obrigatoriedade de todos os utilizadores definirem palavras-passe fortes, como se descreve abaixo.

Condição	Descrição
Letras do alfabeto latino	Inclua uma mistura de caracteres maiúsculos e minúsculos
Números	Inclua pelo menos um número
Caracteres especiais	Inclua pelo menos um carácter especial (por exemplo, <INSCREVA CARACTERES ESPECIAIS AQUI>)
Evite repetições	Não utilize caracteres repetidos (por exemplo, AAA ou 111)
Exclua o nome do utilizador	Não utilize o nome de utilizador em qualquer parte da palavra-passe, incluindo em sentido inverso. Por exemplo, se o nome do utilizador for: user1 e a palavra-passe for: 1resu.
Comprimento mínimo	Recomenda-se a utilização de uma palavra-passe de pelo menos 8 caracteres. O comprimento máximo da palavra-passe é de 64 caracteres.

Além da utilização de palavras-passe fortes, os utilizadores devem também alterá-las periodicamente. Pode especificar o número de dias em que a palavra-passe de um utilizador se mantém válida nas definições do sistema.

As atualizações de software são importantes

A execução de software desatualizado no seu NAS e noutros dispositivos em rede coloca toda a sua rede em risco. A equipa de desenvolvimento da QNAP monitoriza e corrige ativamente potenciais vulnerabilidades de segurança, imediatamente quando são descobertas e lança atualizações para o sistema operativo e aplicações com a maior brevidade possível. Recomendamos que os utilizadores mantenham as suas aplicações atualizadas no App Center e que também permitam atualizações automáticas na secção Atualização de Firmware do sistema QTS. O website da QNAP contém Notas de Lançamento que fornecem informações sobre correções e melhoramentos realizados em novas versões de software.

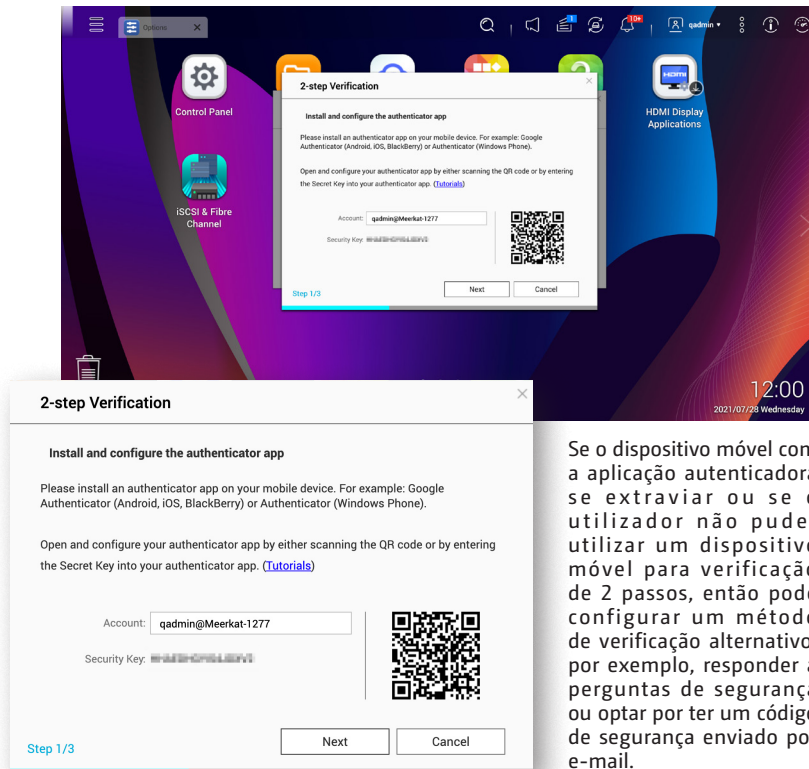


A partir do QTS 4.5.3, o App Center atualizará automaticamente aplicações com novas versões por predefinição (NAS que não podem atualizar para além do QTS 4.5.3 podem permitir atualizações automáticas usando a interface da consola). Se o seu NAS não estiver ligado à Internet, pode descarregar atualizações a partir do Centro de Transferências QNAP e depois instalá-las manualmente no seu NAS.

Ativar a verificação de 2 passos

A verificação de 2 passos aumenta consideravelmente a segurança das contas dos utilizadores. Quando ativado, será solicitado aos utilizadores que introduzam um código de uma aplicação autenticadora no seu dispositivo móvel antes de poderem terminar o início de sessão na sua conta. Isto acrescenta uma camada extra de segurança às contas de utilizador, o que pode reduzir grandemente o potencial dos hackers de acederem ilegalmente a contas do utilizador.

Para utilizar a verificação de 2 passos, deve instalar uma aplicação de verificação no seu dispositivo móvel. Esta aplicação deve usar um algoritmo de palavra-passe monouso por tempo limitado (time-based one-time password - TOTP) para criar um serviço de autenticação. O QTS suporta o Google Authenticator (Android, iOS e BlackBerry) e o Authenticator (Windows Phone) para verificação de 2 passos.



Se o dispositivo móvel com a aplicação autenticadora se extraviar ou se o utilizador não puder utilizar um dispositivo móvel para verificação de 2 passos, então pode configurar um método de verificação alternativo, por exemplo, responder a perguntas de segurança ou optar por ter um código de segurança enviado por e-mail.

Deixe-nos avaliar a segurança para si

Existem riscos de segurança inerentes quando se liga qualquer dispositivo à Internet, razão pela qual a QNAP disponibilizou a aplicação Security Counselor. Esta aplicação audita as potenciais vulnerabilidades de segurança do seu NAS e fornece recomendações para ajustes de configuração do sistema para evitar que o seu NAS seja comprometido.

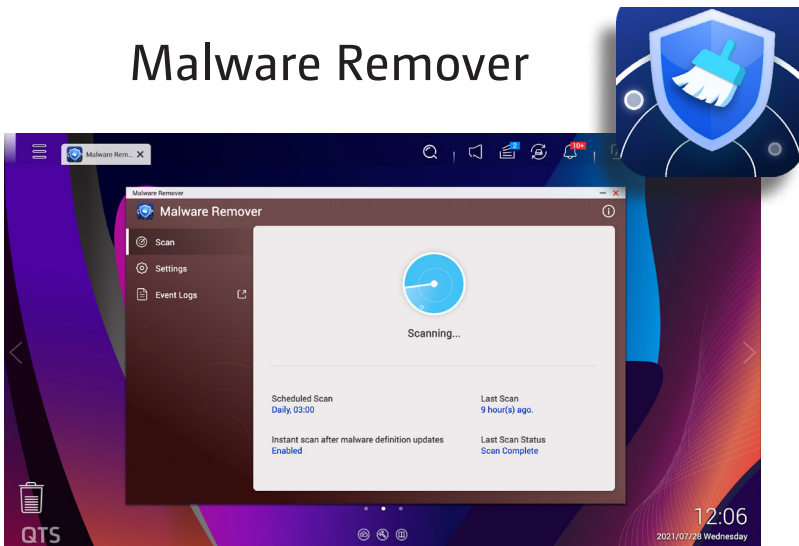
Na Security Counselor, pode especificar diferentes recomendações de nível de segurança com base nos requisitos de utilização do NAS. Também podem ser realizadas análises com base num agendamento. Pode, ainda, ajustar outras definições incluindo bloqueio de IP, credenciais de segurança e políticas de palavra-passe.



Remover instantaneamente as ameaças

As análises regulares podem ser úteis para verificar se o seu NAS foi afetado por malware, com a remoção de malware detetado. O Malware Remover também descarrega automaticamente as definições de malware mais recentes para lhe proporcionar a maior proteção contra ameaças novas e emergentes de malware.

Malware Remover



Também pode configurar os resultados da análise do Malware Remover para serem enviados para a QNAP, permitindo-nos atualizar as nossas definições de malware e ajudar a reforçar a segurança de todos os utilizadores do NAS da QNAP.

Instalar uma firewall de segurança para o NAS

As ameaças à segurança das redes não diferenciam entre redes internas e externas e as firewalls (boundary) baseadas em redes estabelecidas no limite das redes locais são insuficientes para garantir uma segurança global. Atualmente, o conceito de Zero Trust Networks (Redes de Confiança Zero) está a tornar-se generalizado e pode instalar e ativar a QuFirewall em dispositivos QNAP para criar uma firewall baseada no anfitrião (micro-boundary) para proteger os seus serviços e dados críticos.

QuFirewall



A QuFirewall é uma aplicação NAS da QNAP gratuita que lhe permite definir regras de tráfego de rede de entrada para permitir/recusar ligações e melhorar a segurança dos NAS ligados à Internet. A QuFirewall também suporta GeoIP, que pode ser utilizado para detetar e recusar ligações de regiões geográficas especificadas. Para uma proteção ainda maior, pode considerar a instalação da popular firewall de código aberto pfSense do mercado de Máquinas Virtuais da Virtualization Station.

Não deixe o seu NAS exposto

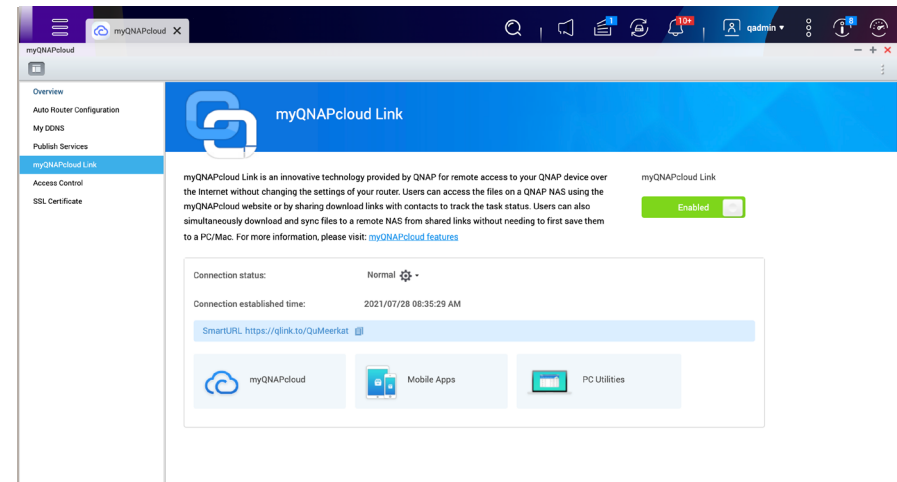
O seu NAS da QNAP é potencialmente vulnerável a ser "espiado" se for ligado diretamente à Internet desprotegido. Ao utilizar botnets ou websites como o Shodan, os atacantes podem potencialmente bloquear dispositivos e lançar ataques. Isto é controlado nas definições de reencaminhamento de porta de routers e modems. Se ativar o reencaminhamento manual, o reencaminhamento automático de portas (UPnP; Universal Plug and Play) ou a zona desmilitarizada (DMZ), o seu NAS da QNAP fica diretamente ligado à Internet. A ligação direta à Internet também ocorre quando o NAS da QNAP obtém diretamente um endereço IP público (estático/PPPoE/DHCP).

Quando precisar de aceder remotamente ao seu NAS, a forma mais segura é estabelecer uma ligação VPN segura ou utilizar a aplicação myQNAPcloud Link. Se não utilizar estes métodos de ligação, deve instalar o NAS da QNAP atrás do seu router e firewall. Se o NAS estiver atrás de um router mas estiver ligado à Internet através do reencaminhamento de portas, deve especificar um novo número de porta no router. Não utilize números de porta como 22, 443, 80, 8080 ou 8081.

Sugestões de segurança para ligações remotas

Uma das melhores coisas sobre o NAS é o acesso universal aos seus ficheiros e serviços a partir de qualquer dispositivo, em qualquer altura. Para tornar a ligação remota mais fácil e mais segura, desenvolvemos a aplicação myQNAPcloud Link, que se liga ao seu NAS (através de ligação P2P) para que possa ligar-se em segurança ao NAS sem necessitar de configurações de firewall extra ou expor diretamente o NAS.

A ligação remota através de serviços DDNS exige habitualmente enfadonhos processos de configuração, mas o myQNAPcloud Link fornece uma ligação remota simples que lhe permite ligar-se ao seu NAS da QNAP onde quer que esteja, tal como se o estivesse a transportar consigo.

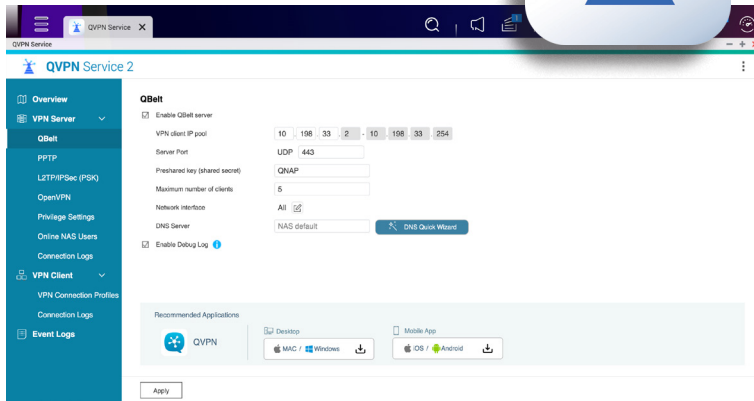


Estabelecer uma ligação VPN segura

Além da ligação remota myQNAPcloud Link, a configuração do seu próprio servidor Virtual Private Network (VPN - Rede privada virtual) no seu NAS da QNAP utilizando o Serviço QVPN proporciona um nível mais elevado de ligação segura que permite uma comunicação mais segura entre os seus dispositivos e o NAS. Além disso, também pode ligar o NAS da QNAP a outros servidores VPN.

QBelt, o protocolo VPN exclusivo QVPN da QNAP, pode reduzir ainda mais a hipótese de serem detetadas ligações VPN. Um computador ou dispositivo móvel pode utilizar o QVPN Device Client para se ligar ao servidor VPN no NAS da QNAP ou ao serviço QuWAN.

Serviço QVPN



Recursos de segurança incorporados

Além das muitas aplicações de reforço da segurança acima mencionadas, os sistemas operativos NAS da QNAP (QTS e QuTS hero) têm uma vasta gama de configurações de segurança incorporadas para adicionar camadas extra de proteção ao seu NAS.

- **Lista Negra e Lista de Permissões de IP:** Utilize a lista de permissões para restringir as ligações apenas a endereços IP autorizados, enquanto que a lista negra pode ser utilizada para bloquear automaticamente a ligação de alguns endereços IP ao NAS.
- **Bloqueio automático:** Configure o seu NAS para bloquear utilizadores/endereços IP que tenham falhado o início de sessão após um número especificado de tentativas. Isto é útil para prevenir ataques de força bruta e garantir a segurança do dispositivo.
- **Ligação HTTPS:** Ative uma ligação HTTPS ao NAS e pode optar por encriptar a sua ligação com um certificado auto-assinado/myQNAPcloud/Let's Encrypt TLS para garantir uma maior segurança.
- **Soluções de cópias de segurança múltiplas** Crie uma cópia de segurança completa do seu NAS de múltiplas formas, incluindo com instantâneos e cópia de segurança/sincronização para um servidor remoto ou serviço de armazenamento em nuvem.
- **Controlo de permissões:** Além dos controlos de segurança da informação, a definição de permissões de pastas concede aos utilizadores mais privacidade, o que não só garante a segurança da informação confidencial, mas também cumpre os requisitos regulamentares.
- **Registos e notificações:** O sistema possui registos de eventos e notificações completas integrados, garantindo a rastreabilidade detalhada das operações e poupando tempo para a manutenção das TI.



Remover riscos desconhecidos

As contas de utilizador devem ser monitorizadas e modificadas com base nas suas necessidades. Deve remover as contas que já não são necessárias ou revogar todas as suas permissões se a conta for necessária mais tarde. Pode fazê-lo a partir de "Painel de Controlo" > "Permissões" > "Utilizadores". Também deve monitorizar quais as aplicações que os utilizadores têm instaladas e verificar se são necessárias depois de uma conta de utilizador ser removida. Se, em algum momento, encontrar uma conta de utilizador que não reconheça ou não se lembre de ter criado, então deve ser removida imediatamente.

Instalar software antivírus

Além do antivírus gratuito ClamAV integrado no QTS, também pode adquirir o McAfee Antivirus, um conhecido software antivírus, para proteção avançada. Os utilizadores da QNAP podem fazer análises manuais ou agendadas para proteger os seus dados contra vírus, reparar ficheiros infetados, colocar em quarentena ficheiros infetados e receber as últimas definições de vírus para se protegerem contra vírus novos e emergentes. As licenças McAfee Antivirus podem ser adquiridas na QNAP Software Store com durações de até 3 anos.

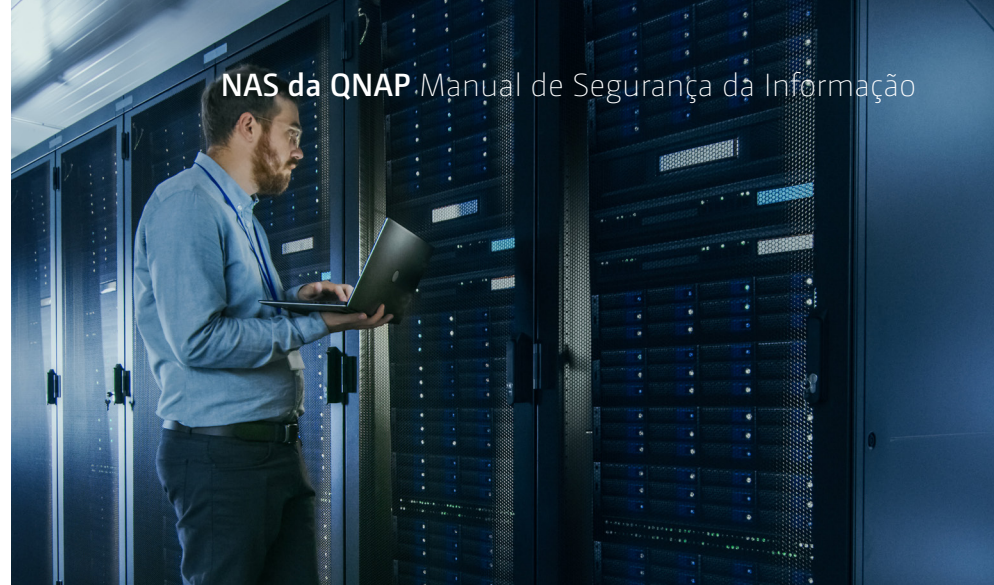
Essential	Pro	Premium
Subscrição Anual Antivírus para NAS	Subscrição Semestral Antivírus para NAS	Subscrição Quadrimestral Antivírus para NAS
USD \$25.00 /Ano	USD \$50.00 /2 Anos	USD \$70.00 /3 Anos
SUBSCREVER AGORA	SUBSCREVER AGORA	SUBSCREVER AGORA

A equipa de segurança da QNAP está em estado de vigília 24 horas por dia

A QNAP foi certificada em 2018 pela MITRE, uma organização internacional sem fins lucrativos, como Autoridade de Numeração CVE. Isto permite à QNAP atribuir identificadores CVE para questões de segurança nos produtos da QNAP. A Equipa de Resposta a Incidentes de Segurança de Produtos da QNAP (PSIRT - Product Security Incident Response Team) recebe notificações de segurança de informação em tempo real de todo o mundo, investiga proativamente vulnerabilidades, revela publicamente ameaças e responde a notificações de vulnerabilidade no prazo de 24 horas após a sua receção.

Recomendamos que os utilizadores verifiquem regularmente o Boletim de Segurança da Informação da QNAP e que subscrevam a respetiva newsletter para obterem as informações e atualizações mais recentes. No caso de um incidente de segurança, siga as práticas recomendadas pela equipa PSIRT da QNAP para ajudar a evitar que um incidente de segurança comprometa o seu NAS.

Advisory	Status	Impact	CVE	Last Updated	Affected Product(s)
<p>Improper Access Control Vulnerability in Legacy HBS 3 (Hybrid Backup Sync)</p> <p>QNAP SA ID: QSA-21-19</p> <p>First Published: 2021-07-06</p> <p>Summary: An improper access control vulnerability has been reported to affect certain legacy versions of HBS 3 (Hybrid Backup Sync). If exploited, this vulnerability allows attackers to compromise the security of the operating system. We have already fixed this vulnerability in the following versions of HBS 3 QTS 4.3.6...</p> <p>Learn More</p>	Resolved	Critical	CVE-2021-28809	2021-07-06	Certain QNAP NAS
Multiple Command Injection Vulnerabilities in QTS and QuTS hero	Resolved	Medium	CVE-2021-28802 CVE-2021-28804	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in QuLog Center	Resolved	Medium	CVE-2020-36196	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in Q'center	Resolved	Medium	CVE-2021-28803	2021-06-25	Certain QNAP NAS
XSS Vulnerability in QTS and QuTS hero	Resolved	Medium	CVE-2020-36194	2021-06-25	Certain QNAP NAS
DNSpoof Vulnerabilities in QTS	Resolved	Medium	CVE-2020-25684 CVE-2020-25685 CVE-2020-25686	2021-06-28	Certain QNAP NAS



Como devo proceder se o meu NAS for atingido por um ataque de encriptação?

Os ataques ransomware podem variar nos seus efeitos e vetores de ataque, por isso é difícil definir uma resposta geral recomendada para um ataque. Para se preparar contra potenciais ataques, recomendamos vivamente que siga as melhores práticas para criar cópias de segurança e recuperação de desastres: cópias de segurança diárias, guardar cópias de segurança em múltiplos dispositivos, utilizar instantâneos e cópias de segurança de instantâneos. Recorde também que deve subscrever a newsletter de segurança da informação da QNAP para receber as últimas atualizações.

Se suspeitar que o seu NAS ou outros dispositivos em rede foram comprometidos (por exemplo, uma utilização anormalmente elevada da CPU causada por aplicações/serviços desconhecidos, falhas no início de sessão, ficheiros desconhecidos em pastas ou encriptação não autorizada de ficheiros) então deverá remover imediatamente o seu NAS da rede e desligar a sua rede da Internet. O seu NAS deve então ser imediatamente encerrado* e deve contactar o QNAP Helpdesk para obter mais informações. Também deve verificar a integridade das suas cópias de segurança e verificar a eventualidade de terem ficado comprometidas.

A aplicação Malware Remover pode ser utilizada para limpar o malware eventualmente existente no seu sistema. Certifique-se de que está a utilizar a versão mais recente do Malware Remover.

Se estiver a utilizar instantâneos e tiver confirmado que os seus ficheiros de instantâneos não estão afetados, pode usar a função de recuperação de instantâneo para recuperar os seus dados valiosos.

* Na maior parte dos casos, a melhor prática é encerrar imediatamente o NAS quando é detetado um ataque pela primeira vez. São poucos os ataques de encriptação que podem fazer com que o NAS perca a chave de descriptação após o encerramento. Os utilizadores são aconselhados a prestar atenção ao Boletim de Segurança da Informação da QNAP.

A segurança da informação é a prioridade máxima da QNAP

O compromisso da QNAP com a segurança da informação é intransigente. Mantemos ativamente a segurança da informação e combinamos os pontos fortes dos nossos parceiros e da comunidade para garantir a segurança dos produtos QNAP para a sua paz de espírito.

QNAP SYSTEMS, INC.

TEL: +886-2-2641-2000 FAX: +886-2-2641-0555 E-mail: qnapsales@qnap.com

Morada: 3F, No.22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221, Taiwan

A QNAP pode efetuar alterações às especificações e descrições dos produtos em qualquer altura, sem aviso prévio.
Copyright © 2021 QNAP Systems, Inc. Todos os direitos reservados.

QNAP® e outros nomes de QNAP Products são marcas de propriedade ou marcas comerciais registadas da QNAP Systems, Inc.
Outros nomes de produtos e de empresas aqui mencionados são marcas comerciais dos seus respetivos titulares.

Países Baixos (Serviços de Armazém)

E-mail: nlsales@qnap.com
TEL: +31(0)107600830

China

E-mail: cnsales@qnap.com
TEL: +86-400-028-0079

Japão

E-mail: jpsales@qnap.com
FAX: 03-6435-9686

EUA

E-mail: usasales@qnap.com
TEL: +1-909-595-2782

Índia

E-mail: indiasales@qnap.com

França

E-mail: frsales@qnap.com

Tailândia

E-mail: thsales@qnap.com
TEL: +66-2-5415988

Alemanha

E-mail: desales@qnap.com