

# QNAP NAS

Manuale sulla sicurezza delle informazioni

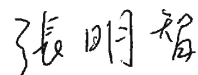


QNAP SYSTEMS, INC.

Grazie per aver utilizzato i prodotti QNAP e per aver affidato la sicurezza dei dati a QNAP NAS. Apprezziamo molto il suo sostegno e consideriamo la sua fiducia la risorsa più preziosa. A tal fine ci impegniamo per la perfezione migliorando costantemente i nostri prodotti e la sicurezza fornita.

Nel mondo di oggi, con un numero crescente di attacchi, malware e problemi di sicurezza, abbiamo sentito il bisogno di fornirvi le seguenti informazioni per aiutarvi a tutelare la vostra identità ed i vostri asset digitali. Ci auguriamo che, grazie ai consigli di questa guida e alle corrette abitudini di utilizzo IT, tutti gli utenti possano proteggere i propri dispositivi e dati dalle minacce correnti e da quelle future.

QNAP Systems, Inc.



Direttore generale

[www.qnap.com](http://www.qnap.com)

## Best practice per migliorare la sicurezza

I metodi di protezione dei dati vengono indirizzati costantemente all'aggiornamento con le tecniche di hacking in continua evoluzione. Per mantenere protetti i dati e i dispositivi, gli utenti NAS dispongono di molti strumenti, tra cui protezione tramite password, impostazioni di autorizzazione, crittografia a livello di file, aggiornamenti del sistema operativo e del software, impostazioni di connessione di rete e app per il backup dei dati e ripristino di emergenza. I prodotti QNAP sono dotati di funzioni di sicurezza di informazioni solide e di vario tipo. Di seguito sono riportati nove (9) punti sulla sicurezza delle informazioni che consentono agli utenti di acquisire rapidamente una conoscenza di base della sicurezza delle informazioni.

1. Rimuovere gli account utente sconosciuti o sospetti
2. Rimuovere le applicazioni NAS sconosciute o utilizzate raramente
3. Disattivare le impostazioni automatiche del router in myQNAPcloud
4. Impostare i controlli di accesso al dispositivo
5. Non rivelare il numero di porta predefinito su Internet
6. Installare ed eseguire la versione più recente di Malware Remover
7. Modificare regolarmente le password di ogni account utente
8. Aggiornare le applicazioni installate alle versioni più recenti
9. Verificare che il sistema operativo e/o il software di sistema dei dispositivi collegati in rete siano sempre aggiornati

In seguito, illustreremo i vari progetti di sicurezza delle informazioni di QNAP uno alla volta e costruiremo ulteriormente un piano di difesa NAS completo.

## Utilizzare password complesse

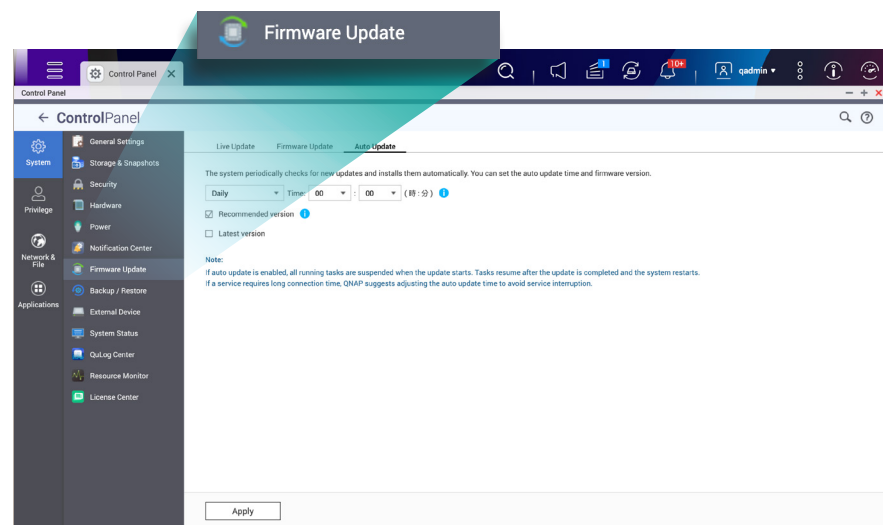
Il tentativo di accedere all'account di un utente è il vettore di attacco più comune per gli hacker. Questa operazione viene solitamente eseguita da hacker che inseriscono password di default o comuni, o utilizzando il social engineering (ad esempio, se viene usato il nome di un animale domestico o di un bambino come password, qualcuno potrebbe indovinarlo). Per ridurre il rischio che un account utente venga compromesso, si consiglia di disattivare l'account admin predefinito e di indicare a tutti gli utenti di impostare password complesse, come descritto di seguito.

Condizione	Descrizione
Lettere inglesi	Includere una combinazione di caratteri maiuscoli e minuscoli
Numeri	Includere almeno un numero
Caratteri speciali	Includere almeno un carattere speciale (ad esempio <AGGIUNGI CARATTERI SPECIALI QUI>)
Evitare ripetizioni	Non utilizzare caratteri ripetuti (ad esempio AAA o 111)
Escludere il nome utente	Non utilizzare il nome utente in nessun punto della password, inclusa la versione precedente. Ad esempio, il nome utente è: W user1 e la password è: 1 reu.
Lunghezza minima	Si consiglia di utilizzare una password di almeno 8 caratteri. La lunghezza massima della password è 64 caratteri.

Oltre a utilizzare password complesse, gli utenti devono anche modificarle periodicamente. È possibile specificare il numero di giorni di validità della password di un utente nelle impostazioni di sistema.

## Gli aggiornamenti software sono importanti

L'esecuzione di software non aggiornato sul NAS e su altri dispositivi collegati in rete mette a rischio l'intera rete. Il team di sviluppo QNAP monitora e raggruppa attivamente le potenziali vulnerabilità della sicurezza non appena vengono rilevate e rilascia gli aggiornamenti per il sistema operativo e le app il prima possibile. Si consiglia di mantenere aggiornate le applicazioni in App Center e di abilitare gli aggiornamenti automatici nella sezione aggiornamento firmware del sistema QTS. Il sito Web QNAP contiene le Note di rilascio che forniscono informazioni sulle correzioni e sui miglioramenti apportati alle nuove versioni software.

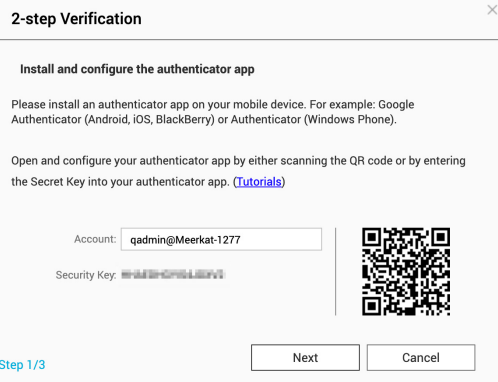
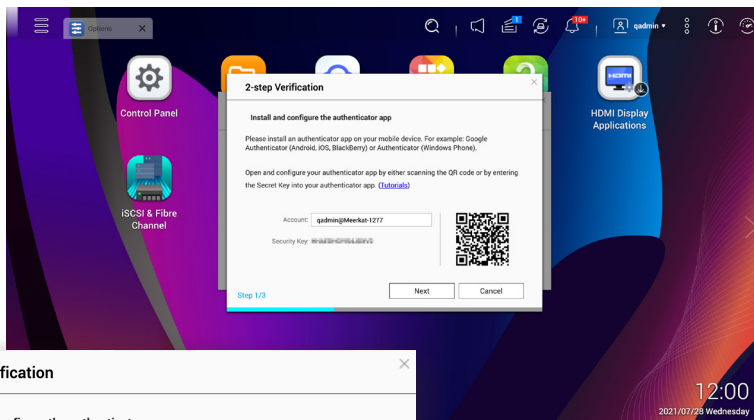


A partire da QTS 4.5.3, l'App Center aggiorna automaticamente le app con nuove versioni per impostazione predefinita (i NAS che non possono eseguire l'aggiornamento oltre QTS 4.5.3 possono abilitare gli aggiornamenti automatici utilizzando l'interfaccia della console). Se il NAS non è connesso a Internet, è possibile scaricare gli aggiornamenti dall'Area download QNAP e quindi installarli manualmente sul NAS.

## Attivare la verifica in 2 passaggi

La verifica in 2 passaggi migliora notevolmente la protezione degli account utente. Con questa opzione attivata, agli utenti verrà richiesto di immettere un codice da un'app di autenticazione sul dispositivo mobile prima di poter completare l'accesso all'account. Questo aggiunge un ulteriore livello di protezione agli account utente, consentendo di ridurre notevolmente il potenziale degli hacker di accedere agli account utente in modo illecito.

Per utilizzare la verifica in 2 passaggi, è necessario installare un'app di verifica sul dispositivo mobile. Questa applicazione deve utilizzare un algoritmo TOTP (One-Time Password) basato sul tempo per creare un servizio di autenticazione. QTS supporta Google Authenticator (Android, iOS e BlackBerry) e Authenticator (Windows Phone) per la verifica in 2 passaggi.



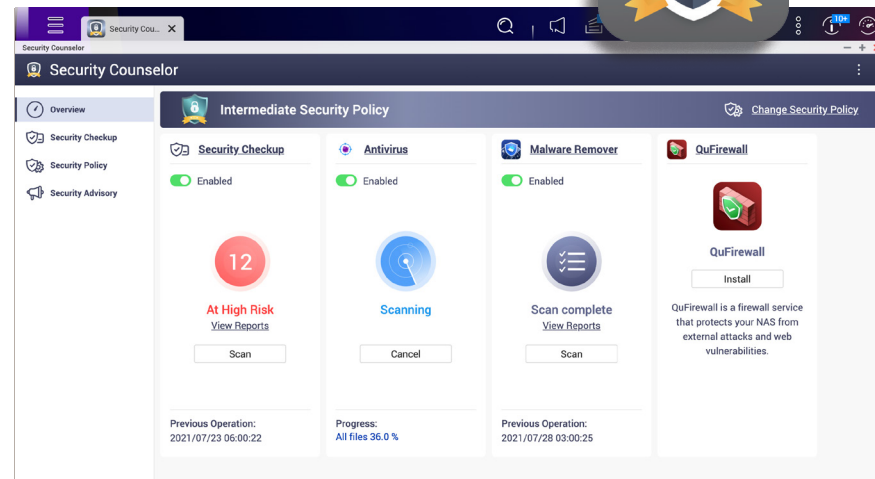
In caso di smarrimento del dispositivo mobile con l'app di autenticazione oppure se l'utente non può utilizzare un dispositivo mobile per la verifica in 2 passaggi, è possibile impostare un metodo di verifica alternativo, ad esempio rispondere a domande di sicurezza o scegliere di inviare un codice di sicurezza tramite e-mail.

## QNAP aiuta a valutare la sicurezza per i suoi utenti

La connessione di un dispositivo a Internet comporta rischi intrinseci per la sicurezza, motivo per cui QNAP ha fornito l'app Security Counselor. Questa app controlla le potenziali vulnerabilità della sicurezza sul NAS e fornisce consigli per le regolazioni della configurazione del sistema per evitare che il NAS venga compromesso.

In Security Counselor è possibile specificare diversi livelli di sicurezza consigliati in base ai requisiti di utilizzo NAS. Le scansioni possono anche essere eseguite su base programmata. È inoltre possibile regolare altre impostazioni, tra cui il blocco IP, le credenziali di protezione e i criteri delle password.

### Security Counselor

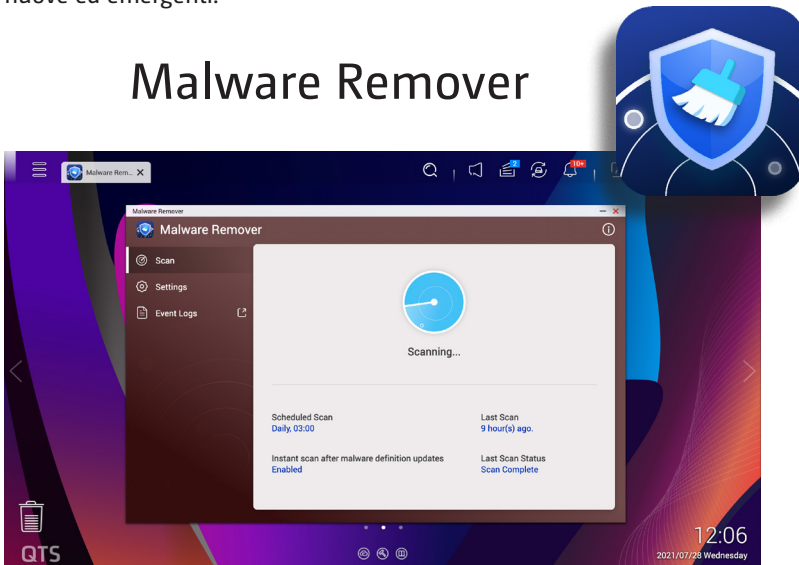




## Rimuovere immediatamente le minacce

Le scansioni regolari possono essere utili per verificare se il NAS è stato interessato da malware, con il malware rilevato rimosso. Malware Remover scarica inoltre automaticamente le definizioni di malware più recenti per offrire la massima protezione contro le minacce di malware nuove ed emergenti.

### Malware Remover



È inoltre possibile configurare i risultati della scansione di malware Remover da inviare a QNAP, consentendoci di aggiornare le definizioni di malware e di contribuire a rafforzare la sicurezza di tutti gli utenti QNAP NAS.

## Installare un firewall di sicurezza per il NAS

Le minacce alla sicurezza in rete non differenziano le reti interne ed esterne, mentre i firewall (boundary) basati sulla rete impostati ai margini delle reti locali non sono sufficienti a garantire una protezione completa. Attualmente, il concetto di reti Zero Trust sta diventando mainstream ed è possibile installare e abilitare QuFirewall sui dispositivi QNAP per creare un firewall basato su host (micro-boundary) per proteggere i dati e i servizi critici.

### QuFirewall



QuFirewall è un'applicazione NAS QNAP gratuita che consente di impostare le regole del traffico di rete in entrata per consentire/negare le connessioni e migliorare la sicurezza del NAS connesso a Internet. QuFirewall supporta inoltre GeoIP, che può essere utilizzato per rilevare e negare connessioni da determinate aree geografiche. Per una protezione ancora maggiore, è possibile installare il famoso firewall open source pfSense dal Virtual Machine Marketplace di Virtualization Station.

## Non lasciare il NAS esposto

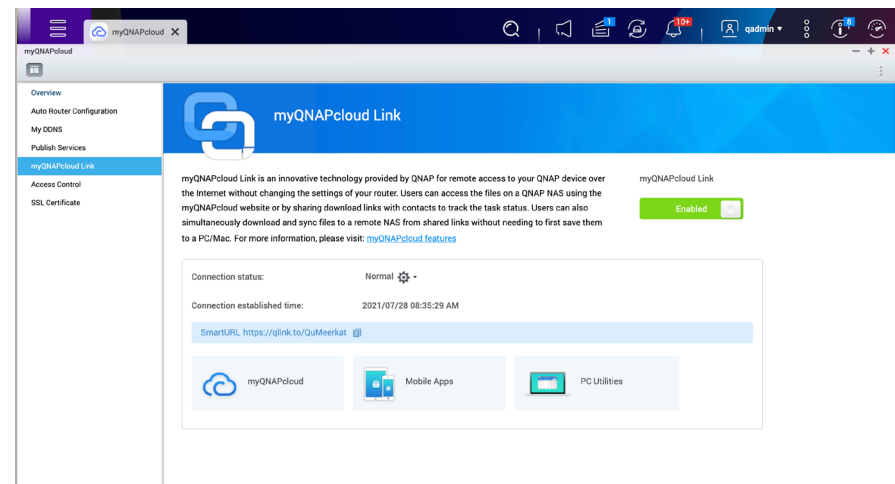
Il NAS QNAP è potenzialmente vulnerabile allo snooping se si connette direttamente a Internet senza protezione. Utilizzando botnet o siti Web come Shodan, utenti malintenzionati possono potenzialmente bloccare i dispositivi e lanciare attacchi. Questo rischio viene controllato attraverso impostazioni di inoltramento delle porte di router e modem. Se si attiva l'inoltramento manuale, l'inoltramento automatico delle porte (UPnP; Universal Plug and Play) o la zona demilitarizzata (DMZ), allora il vostro NAS QNAP è collegato direttamente a Internet. La connessione diretta a Internet avviene anche quando il NAS QNAP ottiene direttamente un indirizzo IP pubblico (statico/PPPoE/DHCP).

Quando è necessario accedere in remoto al NAS, il modo più sicuro è stabilire una connessione VPN protetta o utilizzare l'applicazione myQNAPcloud link. Se non si utilizzano questi metodi di connessione, è necessario installare il NAS dietro il router e il firewall. Se il NAS è protetto da un router ma è connesso a Internet tramite l'inoltramento delle porte, è necessario specificare un nuovo numero di porta sul router. Non utilizzare numeri di porta come 22, 443, 80, 8080 o 8081.

## Suggerimenti per la protezione delle connessioni remote

Una delle cose migliori del NAS è l'accesso universale ai file e ai servizi da qualsiasi dispositivo in qualsiasi momento. Per rendere la connessione remota più semplice e sicura, abbiamo sviluppato l'applicazione myQNAPcloud link, che si connette al vostro NAS (tramite connessione P2P) in modo da poter connettersi in modo sicuro al NAS senza richiedere impostazioni firewall aggiuntive o esporre direttamente il NAS.

La connessione remota tramite i servizi DDNS richiedeva processi di configurazione noiosi, ma myQNAPcloud link fornisce una semplice connessione remota che consente di connettersi QNAP NAS ovunque ci si trovi, proprio come se lo si stesse portando con sé.

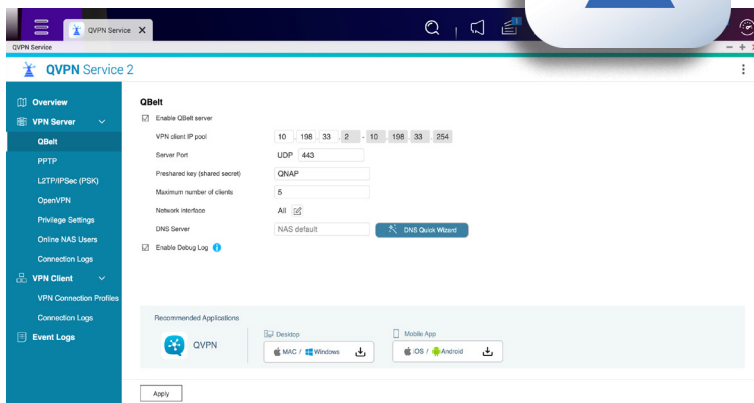


## Stabilire una connessione VPN protetta

Oltre alla connessione remota myQNAPcloud link, la configurazione del proprio server VPN (Virtual Private Network) sul QNAP NAS utilizzando il servizio QVPN fornisce un livello più elevato di connessione sicura che consente una comunicazione più sicura tra i dispositivi e il NAS. Inoltre, è possibile collegare QNAP NAS ad altri server VPN.

QBelt, il protocollo VPN esclusivo QNAP, è in grado di ridurre ulteriormente la possibilità di rilevare connessioni VPN. Un computer o un dispositivo mobile può utilizzare QVPN Device Client per connettersi al server VPN sul QNAP NAS o al servizio QuWAN.

### Servizio QVPN



## Funzioni di sicurezza integrate

Oltre alle numerose applicazioni per il miglioramento della sicurezza menzionate in precedenza, i sistemi operativi NAS di QNAP (QTS e QuTS Hero) dispongono di un'ampia gamma di impostazioni di sicurezza integrate per aggiungere livelli di protezione aggiuntivi al NAS.

- **Blacklist e whitelist IP:** utilizzare la whitelist per limitare le connessioni solo agli indirizzi IP autorizzati, mentre la blacklist può essere utilizzata per bloccare automaticamente la connessione di determinati indirizzi IP al NAS.
- **Blocco automatico:** impostare il NAS per bloccare gli utenti/indirizzi IP che non hanno eseguito l'accesso dopo un numero specificato di tentativi. In questo modo è possibile prevenire attacchi di forza bruta e garantire la sicurezza dei dispositivi.
- **Connessione HTTPS:** attivare una connessione HTTPS al NAS e scegliere di crittografare la connessione con un certificato self-signed/myQNAPcloud/Let's Encrypt TLS per garantire una maggiore sicurezza.
- **Soluzioni di backup multiple:** eseguire il backup completo del NAS in diversi modi, tra cui snapshot e backup/sincronizzazione su un server remoto o un servizio di archiviazione cloud.
- **Controllo autorizzazioni:** oltre ai controlli di sicurezza delle informazioni, l'impostazione delle autorizzazioni per le cartelle garantisce agli utenti una maggiore privacy, garantendo non solo la protezione delle informazioni riservate, ma anche la conformità ai requisiti normativi.
- **Registri e notifiche:** il sistema è dotato di registri eventi e notifiche integrati, che garantiscono una tracciabilità dettagliata delle operazioni e consentono di risparmiare tempo per la manutenzione IT.



## Installare il software antivirus

Oltre all'antivirus gratuito ClamAV integrato in QTS, è possibile acquistare McAfee Antivirus, un noto software antivirus, per una protezione avanzata. Gli utenti QNAP possono eseguire manualmente o pianificare scansioni per proteggere i propri dati dai virus, riparare i file infetti, mettere in quarantena i file infetti e ricevere le più recenti definizioni dei virus per proteggerli da virus nuovi ed emergenti. Le licenze antivirus McAfee possono essere acquistate nel QNAP Software Store con una durata massima di 3 anni.

## Rimuovere rischi sconosciuti

Gli account utente devono essere monitorati e modificati in base alle proprie esigenze. È necessario rimuovere gli account che non sono più necessari o revocarne tutte le autorizzazioni se l'account sarà necessario in un secondo momento. È possibile eseguire questa operazione da "Pannello di controllo" > "Autorizzazioni" > "Utenti". È inoltre necessario monitorare le applicazioni installate dagli utenti e verificare se sono necessarie dopo la rimozione di un account utente. Se, in qualsiasi momento, viene rilevato un account utente sconosciuto o che non presenta alcuna traccia di creazione, allora dovrebbe essere rimosso immediatamente.

## Antivirus McAfee

Eseguire la scansione del NAS per rilevare la presenza di malware manualmente o in base a una pianificazione con il motore antivirus McAfee.

Essenziale	Pro	Premium
Antivirus annuale Abbonamento per NAS	Antivirus - biennale Abbonamento per NAS	Antivirus - triennale Abbonamento per NAS
USD \$25.00 /anno	USD \$50.00 /2 anni	USD \$70.00 /3 anni
ISCRIVITI ORA	ISCRIVITI ORA	ISCRIVITI ORA





## Il team di sicurezza di QNAP è in standby 24 ore su 24

QNAP è stata certificata nel 2018 da MITRE, un'organizzazione internazionale senza scopo di lucro, come CVE Numbering Authority. In tal modo, QNAP può assegnare identificatori CVE per problemi di protezione nei prodotti QNAP. Il Product Security Incident Response Team (PSIRT) di QNAP riceve notifiche in tempo reale sulla sicurezza delle informazioni da tutto il mondo, indaga in modo proattivo sulle vulnerabilità, rivela pubblicamente le minacce e risponde alle notifiche di vulnerabilità entro 24 ore dalla loro ricezione.

Agli utenti viene consigliato di controllare regolarmente le informazioni del QNAP Information Security Bulletin e di iscriversi alla newsletter sulla sicurezza delle informazioni (QNAP Information Security Newsletter) per ottenere le informazioni e gli aggiornamenti più aggiornati. In caso di un incidente di sicurezza, seguire le procedure consigliate dal team PSIRT QNAP per evitare che un incidente di sicurezza comprometta il NAS.

Advisory	Status	Impact	CVE	Last Updated	Affected Product(s)
<p>Improper Access Control Vulnerability in Legacy HBS 3 (Hybrid Backup Sync)</p> <p><b>QNAP SA ID:</b> QSA-21-19</p> <p><b>First Published:</b> 2021-07-06</p> <p><b>Summary:</b> 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><a href="#">Learn More</a></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 QLog 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



## Cosa si deve fare se il NAS viene colpito da un attacco di crittografia?

Gli attacchi ransomware possono variare in termini di effetti e vettori di attacco, pertanto è difficile impostare una risposta generale consigliata a un attacco. Per prepararsi contro potenziali attacchi, si consiglia di seguire le procedure consigliate per il backup e il ripristino di emergenza: Backup giornalieri, salvataggio di backup su più dispositivi, utilizzo di snapshot e backup di snapshot. Inoltre, è importante iscriversi alla newsletter sulla sicurezza delle informazioni di QNAP per ricevere gli aggiornamenti più recenti.

Se si sospetta che il NAS o altri dispositivi di rete siano stati compromessi (ad esempio, un utilizzo eccessivo della CPU causato da applicazioni/servizi sconosciuti, errori di accesso, file sconosciuti nelle cartelle, o la crittografia non autorizzata dei file) sarà opportuno rimuovere immediatamente il NAS dalla rete e disconnettere la rete da Internet. Il NAS deve quindi essere immediatamente spento\* e l'helpdesk QNAP deve essere contattato per ulteriori informazioni. È inoltre necessario verificare l'integrità dei backup e verificare se sono stati compromessi.

L'app malware Remover può essere utilizzata per eliminare potenzialmente il malware dal sistema. Assicurarsi di utilizzare la versione più aggiornata di Malware Remover.

Se si utilizzano snapshot, e se è stato confermato che il file snapshot non è interessato, è possibile utilizzare la funzione di ripristino snapshot per recuperare i dati importanti.

\* Nella maggior parte dei casi, la procedura migliore è spegnere il NAS immediatamente quando viene rilevato un attacco. Solo pochi attacchi di crittografia possono causare la perdita della chiave di decrittografia da parte del NAS dopo lo spegnimento. Si consiglia agli utenti di prestare attenzione al bollettino sulla sicurezza delle informazioni QNAP.



## **La sicurezza delle informazioni è la priorità principale di QNAP**

L'impegno di QNAP nei confronti della sicurezza delle informazioni è senza compromessi. Manteniamo attivamente la sicurezza delle informazioni e uniamo i punti di forza dei nostri partner e della comunità per garantire la sicurezza dei prodotti QNAP per la tranquillità dei nostri clienti.

# QNAP SYSTEMS, INC.

TEL.: +886-2-2641-2000 FAX: +886-2-2641-0555 Email: [qnapsales@qnap.com](mailto:qnapsales@qnap.com)

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

QNAP potrebbe modificare le specifiche e le descrizioni del prodotto in qualsiasi momento senza preavviso.

Copyright © 2021 QNAP Systems, Inc. Tutti i diritti riservati.

QNAP® e altri nomi dei prodotti QNAP sono marchi di proprietà o marchi registrati di QNAP Systems, Inc.

Altri prodotti e nomi societari riportati qui possono essere marchi registrati dei rispettivi proprietari.

## **Paesi Bassi (Servizi di magazzino)**

e-mail: [nlsales@qnap.com](mailto:nlsales@qnap.com)

TEL.: +31(0)107600830

## **Stati Uniti**

e-mail: [usasales@qnap.com](mailto:usasales@qnap.com)

TEL.: +1-909-595-2782

## **Thailandia**

e-mail: [thsales@qnap.com](mailto:thsales@qnap.com)

TEL.: +66-2-5415988

## **Cina**

e-mail: [cnsales@qnap.com](mailto:cnsales@qnap.com)

TEL.: +86-400-028-0079

## **India**

e-mail: [indiasales@qnap.com](mailto:indiasales@qnap.com)

## **Germania**

e-mail: [desales@qnap.com](mailto:desales@qnap.com)

## **Giappone**

e-mail: [jpsales@qnap.com](mailto:jpsales@qnap.com)

FAX: 03-6435-9686

## **Francia**

e-mail: [frsales@qnap.com](mailto:frsales@qnap.com)