

# QNAP NAS

Bilgi Güvenliđi Kılavuzu



QNAP SYSTEMS, INC.

## Güvenliği geliştirmek için en iyi uygulamalar

Veri koruma yöntemleri sürekli olarak gelişen bilgisayar korsanlığı tekniklerine ayak uydurmaya çalışmaktadır. NAS kullanıcıları, verilerini ve aygıtlarını korumak için parola koruması, izin ayarları, dosya düzeyinde şifreleme, işletim sistemi ve yazılım güncellemeleri, ağ bağlantısı ayarları ve veri yedekleme ve acil durumda kurtarma uygulamaları gibi pek çok araca sahiptir. QNAP ürünleri çok yönlü ve sağlam bilgi güvenliği özelliklerine sahiptir. Aşağıda, kullanıcılarımızın bilgi güvenliği konusunda hızlı bir şekilde temel bir anlayış kazanmalarına yardımcı olacak bilgi güvenliği ile ilgili dokuz (9) madde verilmiştir.

1. Bilinmeyen veya şüpheli kullanıcı hesaplarını kaldırın
2. Bilinmeyen veya nadir kullanılan NAS uygulamalarını kaldırın
3. myQNAPcloud'da otomatik yönlendirici ayarlarını devre dışı bırakın
4. Aygıt erişim kontrollerini ayarlayın
5. İnternette varsayılan bağlantı noktası numarasını açıklamayın
6. Malware Remover'ın son sürümünü yükleyip çalıştırın
7. Her kullanıcı hesabının parolasını düzenli aralıklarla değiştirin
8. Yüklenen uygulamaları son sürümlere güncelleyin
9. Ağa bağlı aygıtlarınızın işletim sisteminin ve/veya sistem yazılımının her zaman güncel olduğundan emin olun

Daha sonra, QNAP'in çeşitli bilgi güvenliği tasarımlarını tek tek açıklayacağız ve kapsamlı bir NAS savunma planı oluşturacağız.

QNAP ürünlerini kullandığınız ve verilerinizi korumak amacıyla QNAP NAS'a emanet ettiğiniz için teşekkür ederiz. Desteğiniz için çok teşekkür ederiz ve bize olan güveninizi en değerli varlığımız olarak görüyoruz. Bu amaçla ürünlerimizi ve güvenliğimizi sürekli geliştirerek mükemmellik için çalışıyoruz.

Saldırıların, kötü amaçlı yazılımların ve güvenlik endişelerinin giderek arttığı günümüzde, kendinizi ve dijital varlıklarınızı proaktif bir şekilde korumanıza yardımcı olmak için size aşağıdaki bilgileri sağlama ihtiyacı gördük. Bu kılavuzdaki tavsiyeleri mantıklı BT kullanım alışkanlıklarıyla birleştirerek tüm kullanıcılarımızın aygıtlarını ve verilerini mevcut ve yeni ortaya çıkan tehditlere karşı koruyabileceklerini umuyoruz.

QNAP Systems, Inc.



Genel Müdür

www.qnap.com

## Güçlü parolalar kullanın

Bir kullanıcının hesabına erişmeye çalışmak, bilgisayar korsanlarının en yaygın saldırı vektörüdür. Bu genellikle bilgisayar korsanlarının varsayılan veya yaygın parolaları denemesi veya sosyal mühendislik kullanması yoluyla gerçekleştirilir (örneğin: birisi parola olarak evcil hayvanının veya çocuğunun adını kullandıysa, birisi bunu tahmin edebilir). Bir kullanıcı hesabının ele geçirilmesi tehdidini azaltmak amacıyla, varsayılan yönetici hesabının devre dışı bırakılmasını ve tüm kullanıcıların aşağıda açıklandığı gibi güçlü parolalar belirlemesini zorunlu kılmanızı öneririz.

Şart	Açıklama
İngilizce harfler	Büyük ve küçük harflerin karışımını ekleyin
Sayılar	En az bir sayı ekleyin
Özel karakterler	En az bir özel karakter ekleyin (örneğin <BURAYA ÖZEL KARAKTERLER EKLEYİN>)
Karakter tekrarından kaçının	Tekrarlayan karakterler kullanmayın (AAA veya 111 gibi)
Kullanıcı adını kullanmayın	Kullanıcı adını, tersi de dahil olmak üzere parolanın hiçbir yerinde kullanmayın. Örneğin kullanıcı adı: W user1 ve parola: 1resu
Minimum uzunluk	En az 8 karakterden oluşan bir parola kullanmanız önerilir. Parola için maksimum uzunluk 64 karakterdir.

Güçlü parola kullanmanın yanı sıra, kullanıcılar parolalarını düzenli aralıklarla değiştirmelidir. Sistem ayarlarında bir kullanıcının parolasının geçerli olacağı gün sayısını belirleyebilirsiniz.

## Yazılım güncellemeleri önemlidir

NAS ve diğer ağa bağlı aygıtlarınızda güncel olmayan yazılımların çalıştırılması tüm ağınıza riske atar. QNAP geliştirme ekibi, potansiyel güvenlik açıklarını keşfedilir keşfedilmez aktif olarak izler ve yamalar ve işletim sistemi ve uygulamalar için güncellemeleri mümkün olan en kısa sürede yayınlar. Kullanıcıların Uygulama Merkezinde uygulamalarını güncel tutmalarını ve ayrıca QTS sisteminin Firmware Güncellemesi bölümünde otomatik güncellemeleri etkinleştirmelerini öneririz. QNAP web sitesinde, yeni yazılım sürümlerinde yapılan düzeltmeler ve iyileştirmeler hakkında bilgi sağlayan Sürüm Notları bulunur.

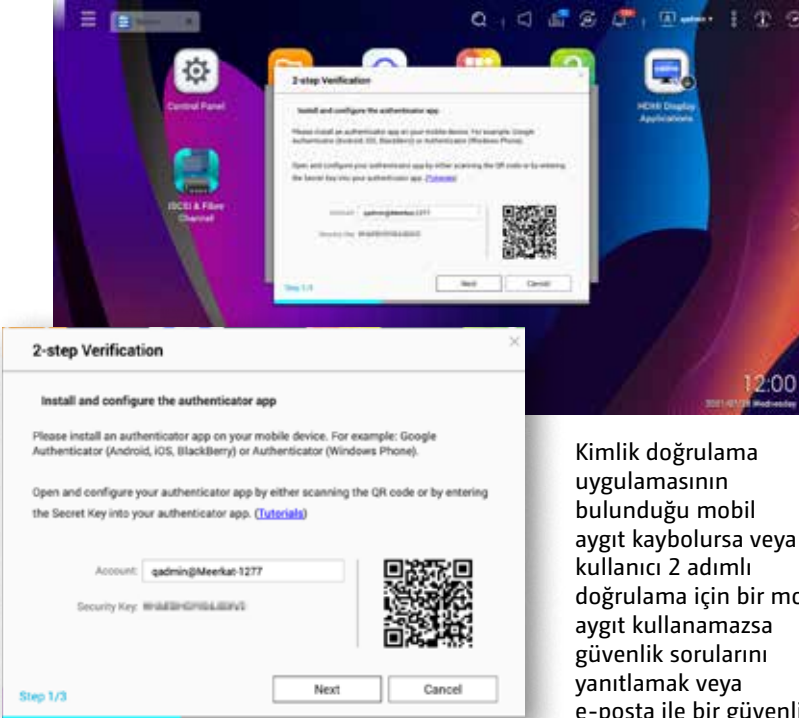


QTS 4.5.3'ten itibaren, Uygulama Merkezi varsayılan olarak uygulamaları yeni sürümlerle otomatik olarak güncelleyecektir (QTS 4.5.3'ün üzerine yükseltme yapılmayan NAS'ta konsol arayüzü kullanılarak otomatik güncellemeler etkinleştirilebilir). NAS'ınız İnternet'e bağlı değilse, güncellemeleri QNAP Download Center'dan indirebilir ve ardından bunları NAS'ınıza manuel olarak yükleyebilirsiniz.

## 2 adımlı doğrulamayı etkinleştirin

2 adımlı doğrulama, kullanıcı hesaplarının güvenliğini büyük ölçüde artırır. Etkinleştirildiğinde, kullanıcılardan hesaplarına giriş yapmayı bitirmeden önce mobil aygıtlarındaki bir kimlik doğrulayıcı uygulamasından bir kod girmeleri istenecektir. Bu, kullanıcı hesaplarına ekstra bir güvenlik katmanı ekleyerek bilgisayar korsanlarının kullanıcı hesaplarına yasa dışı yollardan erişme potansiyelini büyük ölçüde azaltabilir.

2 adımlı doğrulamayı kullanmak için mobil aygıtınıza doğrulama uygulaması yüklemeniz gerekmektedir. Bu uygulama, bir kimlik doğrulama hizmeti oluşturmak için zaman tabanlı tek seferlik parola (TOTP) algoritması kullanmalıdır. QTS, 2 adımlı doğrulama için Google Authenticator (Android, iOS ve BlackBerry) ve Authenticator'ı (Windows Phone) destekler.



Kimlik doğrulama uygulamasının bulunduğu mobil aygıt kaybolursa veya kullanıcı 2 adımlı doğrulama için bir mobil aygıt kullanamazsa güvenlik sorularını yanıtlamak veya e-posta ile bir güvenlik kodu gönderilmesini seçmek gibi alternatif bir doğrulama yöntemi ayarlayabilirsiniz.

## Güvenliği sizin için değerlendirelim

Herhangi bir aygıtı internete bağlarken güvenlik riskleri vardır, bu nedenle QNAP Security Counselor uygulamasını sağlamıştır. Bu uygulama NAS'ınızdaki olası güvenlik açıklarını denetler ve NAS'ınızın tehlikeye girmesini önlemek için sistem yapılandırma ayarlamalarına yönelik öneriler sunar.

Security Counselor'da NAS kullanım gereksinimlerine göre farklı güvenlik düzeyi önerileri belirleyebilirsiniz. Planlı şekilde taramalar da yapılabilir. IP engelleme, güvenlik kimlik bilgileri ve parola ilkeleri gibi diğer ayarları da yapabilirsiniz.

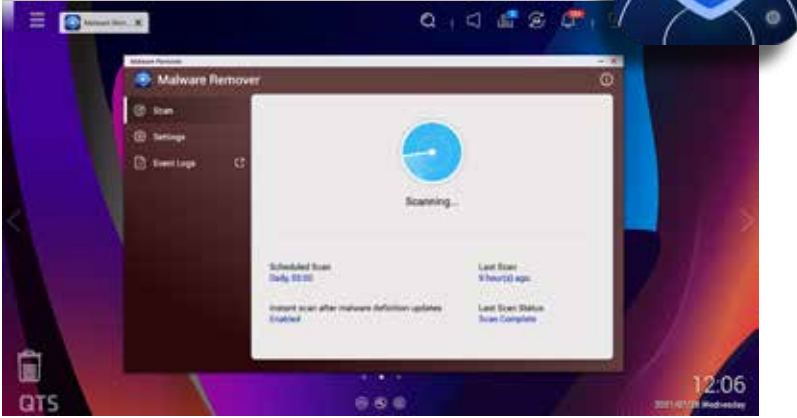
## Security Counselor



## Tehditleri anında kaldırın

NAS'ınızın kötü amaçlı yazılımlardan etkilenip etkilenmediğini görmek için düzenli taramalar yararlı olabilir ve tespit edilen kötü amaçlı yazılımlar kaldırılır. Malware Remover ayrıca yeni ve gelişmekte olan kötü amaçlı yazılım tehditlerine karşı en iyi korumayı sağlamak için en son kötü amaçlı yazılım tanımlarını otomatik olarak indirir.

### Malware Remover

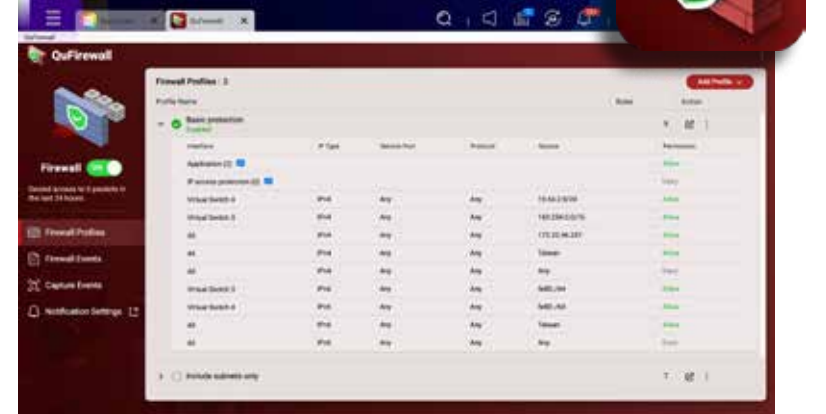


Ayrıca Malware Remover'ın tarama sonuçlarını QNAP'a gönderilecek şekilde yapılandırarak kötü amaçlı yazılım tanımlarımızı güncellememiz ve tüm QNAP NAS kullanıcılarının güvenliğini güçlendirmemize yardımcı olabilirsiniz.

## NAS için bir güvenlik duvarı kurun

Ağa bağlı güvenlik tehditleri iç ve dış ağlar arasında ayrım yapmaz ve yerel ağların ucunda kurulan ağ tabanlı güvenlik duvarları (sınır) çok yönlü güvenliği sağlamada yetersiz kalır. Şu anda, Sıfır Güven Ağları kavramı yaygın hale gelmektedir ve kritik verilerinizi ve hizmetlerinizi korumak için Ana Bilgisayar Tabanlı bir güvenlik duvarı (mikro sınır) oluşturmak üzere QNAP aygıtlarına QuFirewall'u kurabilir ve etkinleştirebilirsiniz.

### QuFirewall



QuFirewall, bağlantılara izin vermek/reddetmek ve İnternet bağlantılı NAS'ın güvenliğini artırmak için gelen ağ trafiği kurallarını ayarlamanıza olanak tanıyan ücretsiz bir QNAP NAS uygulamasıdır. QuFirewall, belirli coğrafi bölgelerden gelen bağlantıları tespit etmek ve reddetmek için kullanılabilen GeolP'yi de destekler. Daha fazla koruma için Virtualization Station'ın Virtual Machine Marketplace'inden popüler açık kaynak güvenlik duvarı pfSense'i yüklemeyi düşünebilirsiniz.

## NAS'ınızı korunmasız bırakmayın

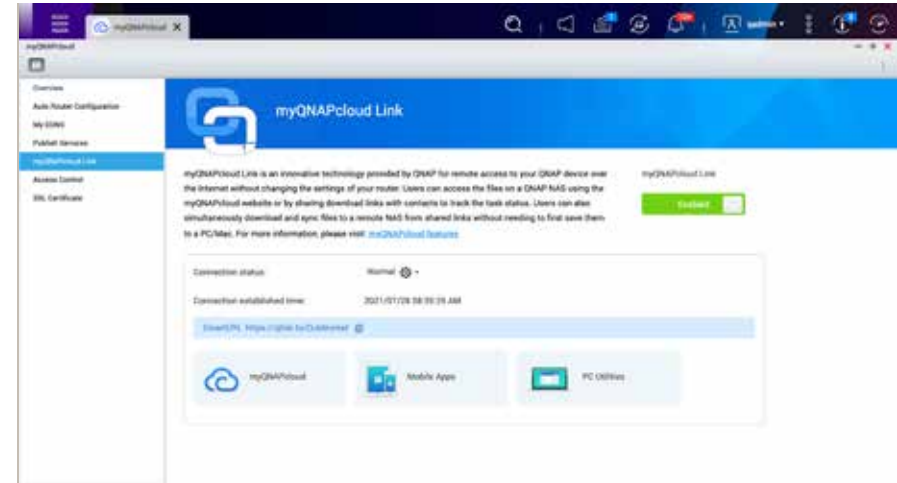
QNAP NAS'ınız korumasız olarak doğrudan İnternete bağlanırsa gözetlemeye karşı potansiyel olarak savunmasız hale gelir. Saldırganlar botnet'leri ya da Shodan gibi web sitelerini kullanarak aygıtları potansiyel olarak kilitleyebilir ve saldırılar başlatabilir. Bu, yönlendiricilerin ve modemlerin bağlantı noktası yönlendirme ayarlarında kontrol edilir. Manuel yönlendirme, otomatik port yönlendirme (UPnP; Evrensel Tak ve Çalıştır) veya savunmasız bölgeyi (DMZ) etkinleştirirseniz QNAP NAS'ınız doğrudan İnternet'e bağlanır. İnternete doğrudan bağlantı, QNAP NAS doğrudan bir genel IP adresi aldığı anda gerçekleşir (statik/PPPoE/DHCP).

NAS'ınıza uzaktan erişmeniz gerektiğinde en güvenli yol güvenli bir VPN bağlantısı kurmak veya myQNAPcloud Link uygulamasını kullanmaktır. Bu bağlantı yöntemlerini kullanmazsanız QNAP NAS'ı yönlendiricinizin ve güvenlik duvarınızın arkasına kurmanız gerekir. NAS bir yönlendiricinin arkasındaysa ancak bağlantı noktası yönlendirme yoluyla İnternete bağlıysa yönlendiricide yeni bir bağlantı noktası numarası belirtmelisiniz. 22, 443, 80, 8080 veya 8081 gibi bağlantı noktası numaralarını kullanmayın.

## Uzaktan bağlantılar için güvenlik ipuçları

NAS ile ilgili en iyi şeylerden biri, dosyalarınıza ve hizmetlerinize herhangi bir aygıttan herhangi bir zamanda evrensel erişimdir. Uzaktan bağlantıyı daha kolay ve daha güvenli hale getirmek için NAS'ınıza (P2P bağlantısı aracılığıyla) bağlanan myQNAPcloud Link uygulamasını geliştirdik, böylece ekstra güvenlik duvarı ayarları gerektirmeden veya NAS'ı doğrudan açığa çıkarmadan NAS'a güvenli bir şekilde bağlanabilirsiniz.

DDNS hizmetleri aracılığıyla uzaktan bağlanmak eskiden sıkıcı kurulum işlemleri gerektiriyordu ancak myQNAPcloud Link, nerede olursanız olun QNAP NAS'ınıza sanki yanınızda taşıyormuşsunuz gibi bağlanabileceğiniz basit bir uzaktan bağlantı sağlar.



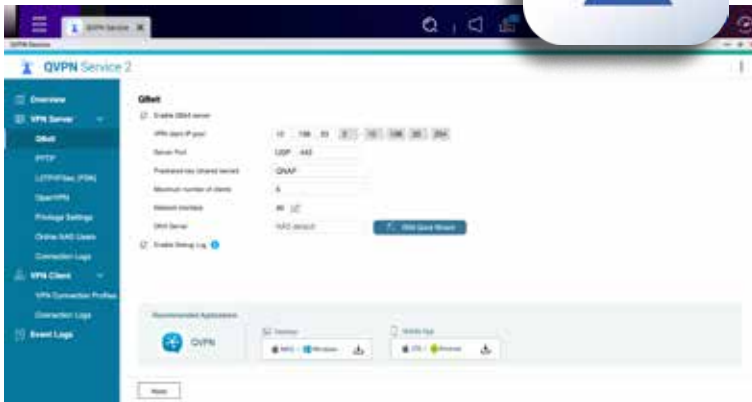


## Güvenli bir VPN bağlantısı kurun

myQNAPcloud Link uzaktan bağlantısına ek olarak QVPN Hizmetini kullanarak QNAP NAS'ınızda kendi Sanal Özel Ağ (VPN) sunucunuzu kurmak, aygıtlarınız ve NAS arasında daha güvenli iletişim sağlayan daha yüksek düzeyde güvenli bir bağlantı sağlar. Ayrıca QNAP NAS'ınızı diğer VPN sunucularına bağlayabilirsiniz.

QNAP'in QVPN'e özel VPN protokolü olan QBelt, VPN bağlantılarının tespit edilme olasılığını daha da azaltabilir. Bir bilgisayar veya mobil aygıt, QNAP NAS üzerindeki VPN sunucusuna veya QuWAN hizmetine bağlanmak için QVPN Aygıt İstemcisini kullanabilir.

### QVPN Hizmeti



## Yerleşik güvenlik özellikleri

Yukarıda belirtilen birçok güvenlik artırma uygulamasına ek olarak QNAP'ın NAS işletim sistemleri (QTS ve QuTS hero) NAS'ınıza ekstra koruma katmanları eklemek için çok çeşitli yerleşik güvenlik ayarlarına sahiptir.

- **IP İçin Kara Liste ve Beyaz Liste:** Bağlantıları yalnızca yetkili IP adresleriyle kısıtlamak için beyaz listeyi kullanın, kara liste ise belirli IP adreslerinin NAS'a bağlanmasını otomatik olarak engellemek için kullanılabilir.
- **Otomatik engelleme:** NAS'ınızı, belirli sayıda denemeden sonra oturum açamayan kullanıcıları/IP adreslerini engelleyecek şekilde ayarlayın. Bu, deneme yanılma saldırılarını önlemek ve aygıt güvenliğini sağlamak için kullanışlıdır.
- **HTTPS bağlantısı:** NAS'a HTTPS bağlantısını etkinleştirin, daha yüksek güvenlik sağlamak için bağlantınızı otomatik imzalı/myQNAPcloud/Let's Encrypt TLS sertifikası ile şifrelemeyi seçebilirsiniz.
- **Çoklu yedekleme çözümleri:** NAS'ınızı snapshot'lar ve uzak bir sunucuya veya bulut depolama hizmetine yedekleme/senkronizasyon dahil olmak üzere çeşitli şekillerde tamamen yedekleyin.
- **İzin Kontrolü:** Bilgi güvenliği kontrollerine ek olarak klasör izinlerinin ayarlanması kullanıcılara daha fazla gizlilik sağlar, bu da yalnızca gizli bilgilerin güvenliğini sağlamakla kalmaz, aynı zamanda yasal gerekliliklere de uygundur.
- **Günlükler ve bildirimler:** Sistemde tam yerleşik olay günlükleri ve bildirimler vardır, bu da işlemlerin ayrıntılı izlenebilirliğini sağlar ve BT bakımı için zaman kazandırır.

## Antivirüs yazılımı yükleyin

QTS'de yerleşik olarak bulunan ücretsiz ClamAV antivirüs yazılımına ek olarak, gelişmiş koruma için tanınmış bir antivirüs yazılımı olan McAfee Antivirus'ü de satın alabilirsiniz. QNAP kullanıcıları, verilerini virüslerden korumak, virüs bulaşmış dosyaları onarmak, virüs bulaşmış dosyaları karantinaya almak ve yeni ve gelişmekte olan virüslere karşı koruma sağlamak için en son virüs tanımlarını almak üzere taramaları manuel olarak yapabilir veya zamanlayabilir. McAfee Antivirüs lisansları QNAP Software Store'dan 3 yıla varan sürelerle satın alınabilir.



## Bilinmeyen riskleri kaldırın

Kullanıcı hesapları izlenmeli ve gereksinimlerinize göre değiştirilmelidir. Artık ihtiyaç duyulmayan hesapları kaldırmalı veya hesaba daha sonra ihtiyaç duyulacaksa tüm izinlerini iptal etmelisiniz. Bunu "Kontrol Paneli" > "İzinler" > "Kullanıcılar" bölümünden yapabilirsiniz. Ayrıca kullanıcıların hangi uygulamaları yüklediğini izlemeli ve bir kullanıcı hesabı kaldırıldıktan sonra bunlara ihtiyaç olup olmadığını doğrulamalısınız. Herhangi bir noktada tanımadığınız veya oluşturduğunuz hatırlamadığınız bir kullanıcı hesabı bulursanız bunu derhal kaldırmanız gerekir.



## QNAP'in güvenlik ekibi günün her saati hazır

QNAP, 2018 yılında kar amacı gütmeyen uluslararası bir kuruluş olan MITRE tarafından CVE Numaralandırma Yetkilisi olarak onaylanmıştır. Bu, QNAP'in QNAP ürünlerindeki güvenlik sorunları için CVE tanımlayıcıları atamasını sağlar. QNAP'in Ürün Güvenliği Olay Müdahale Ekibi (PSIRT), dünyanın dört bir yanından gerçek zamanlı bilgi güvenliği bildirimleri alır, güvenlik açıklarını proaktif olarak araştırır, tehditleri kamuya açıklar ve güvenlik açığı bildirimlerini aldıktan sonra 24 saat içinde yanıtlar.

Kullanıcıların en güncel bilgileri ve güncellemeleri almak için QNAP Bilgi Güvenliği Bültenini düzenli olarak kontrol etmelerini ve QNAP Bilgi Güvenliği Bültenine abone olmalarını tavsiye ederiz. Bir güvenlik olayı durumunda, bir güvenlik olayının NAS'ınızı tehlikeye atmasını önlemeye yardımcı olmak için QNAP PSIRT ekibinin önerdiği uygulamaları izleyin.

Adı	Status	Severity	CVE	Last updated	Affected Product(s)
Improper Access Control Vulnerability in Legacy HBS 3 Hybrid Backup Sync	Resolved	Critical	CVE-2021-28809	2021-07-06	Certain QNAP NAS
<b>QNAP SA ID:</b> QSA-21-19 <b>First Published:</b> 2021-07-06	<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 file, have already fixed this vulnerability in the following versions of HBS 3 QTS 4.3.8...				
1 Multiple Command Injection Vulnerabilities in QTS and QuTS hero	Resolved	Medium	CVE-2021-28802 CVE-2021-28804	2021-06-25	Certain QNAP NAS
2 Stored XSS Vulnerability in Quagmire	Resolved	Medium	CVE-2021-28816	2021-06-25	Certain QNAP NAS
3 Stored XSS Vulnerability in Quagmire	Resolved	Medium	CVE-2021-28803	2021-06-25	Certain QNAP NAS
4 XSS Vulnerability in QTS and QuTS hero	Resolved	Medium	CVE-2021-28814	2021-06-25	Certain QNAP NAS
5 DDoS/DDoS Vulnerabilities in QTS	Resolved	Medium	CVE-2020-25684 CVE-2020-25685 CVE-2020-25686	2021-06-28	Certain QNAP NAS



## NAS'ım bir şifreleme saldırısına maruz kalırsa ne yapmalıyım?

Fidye yazılımı saldırıları etkileri ve saldırı vektörleri bakımından farklılık gösterebilir, bu nedenle bir saldırıya karşı önerilen genel bir yanıt belirlemek zordur. Olası saldırılara karşı hazırlıklı olmak amacıyla yedekleme ve acil durumda kurtarma için en iyi uygulamaları takip etmenizi kesinlikle tavsiye ederiz: günlük yedeklemeler, yedekleri birden fazla aygıtta kaydetme, snapshot'lar ve snapshot yedeklerini kullanma. Ayrıca en son güncellemeleri almak için QNAP'in bilgi güvenliği bültenine abone olmayı unutmayın.

NAS'ınızın veya ağa bağlı diğer aygıtlarınızın ele geçirildiğinden şüpheleniyorsanız (bilinmeyen uygulamaların/hizmetlerin neden olduğu anormal derecede yüksek CPU kullanımı, oturum açma hataları, klasörlerdeki bilinmeyen dosyalar veya dosyaların yetkisiz şifrlenmesi gibi), NAS'ınızı derhal ağınızdan kaldırmalı ve ağınızın İnternet bağlantısını kesmelisiniz. NAS'ınızı derhal kapatılmalı\* ve daha fazla bilgi için QNAP Yardım Masası ile iletişime geçilmelidir. Ayrıca yedeklerinizin bütünlüğünü doğrulamalı ve potansiyel olarak tehlikeye atılıp atılmadıklarını kontrol etmelisiniz.

Malware Remover uygulaması potansiyel olarak kötü amaçlı yazılımları sisteminizden temizlemek için kullanılabilir. Malware Remover'ın en güncel sürümünü kullandığınızdan emin olun.

Snapshot kullanıyorsanız ve snapshot dosyalarınızın etkilenmediğini onayladıysanız, önemli verilerinizi kurtarmak için snapshot kurtarma özelliğini kullanabilirsiniz.

\* Çoğu durumda, bir saldırı ilk tespit edildiğinde NAS'ın hemen kapatılması en iyi uygulamadır. Yalnızca birkaç şifreleme saldırısı NAS'ın kapatıldıktan sonra şifre çözme anahtarını kaybetmesine neden olabilir. Kullanıcıların QNAP Bilgi Güvenliği Bültenine dikkat etmeleri tavsiye edilir.

## Bilgi güvenliđi QNAP'ın en önemli önceliđidir

QNAP'ın bilgi güvenliđine olan bađlılıđı ödün vermez. Bilgi güvenliđini aktif olarak koruyor ve iininizin rahat etmesi iin QNAP ürünlerinin güvenliđini sađlamak üzere ortaklarımızın ve toplumun güçlü yanlarını birleřtiriyoruz.

# QNAP SYSTEMS, INC.

TEL : +886-2-2641-2000 FAKS: +886-2-2641-0555 E-posta: qnapsales@qnap.com

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

QNAP, her zaman bildirimde bulunmaksızın teknik özellikler ve ürün açıklamalarına ilişkin değişiklikler yapabilir.  
Telif Hakkı© 2021 QNAP Systems, Inc. Her hakkı saklıdır.

QNAP® ve QNAP Ürünlerinin diğer adları QNAP Systems, Inc.'nin şahsi markaları veya tescilli ticari markalarıdır.  
Burada bahsi geçen diğer ürünler ve şirket adları ilgili sahiplerinin ticari markalarıdır.

## Hollanda (Depolama Hizmetleri)

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

## ABD

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

## Tayland

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

## Çin

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

## Hindistan

E-posta: indiasales@qnap.com

## Japonya

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

## Fransa

E-posta: frsales@qnap.com

## Almanya

E-posta: desales@qnap.com