Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

QNAP: Proof-of-Concept für Schwachstelle in QNAP QTS, QuTS hero und QuTScloud veröffentlicht

Nr. 2024-213941-1022, Version 1.0, 13.02.2024

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 13. Februar 2024 veröffentlichte der Hersteller QNAP ein Advisory zu mehreren Schwachstellen in den Betriebssystemen QTS, QuTS hero und QuTScloud. Diese kommen in zahlreichen Network Attached Storage (NAS)-Lösungen des Herstellers zum Einsatz. Den Hinweisen des Unternehmens zufolge könnte es Angreifenden gelingen, aus der Ferne ohne Authentifizierung Befehle auf QNAP-Geräten auszuführen [QNAP2024][BSI2024].

Ausschlaggebend hierfür ist zum einen die Schwachstelle CVE-2023-50358, zum anderen die Sicherheitslücke CVE-2023-47218. Beide Verwundbarkeiten wurden nach dem Common Vulnerability Scoring System (CVSS) zwar nur mit einer mittleren Kritikalität (5.8) bewertet, die äußerst hohe Anzahl an über das Internet erreichbaren Geräten - sowohl in Deutschland als auch im Allgemeinen - könnte jedoch zu großen Schäden führen [UNIT2024].

Zusätzlich begünstigt wird diese Bedrohung aufgrund der Tatsache, dass die IT-Sicherheitsforschenden von Unit42 nun Proof of Concept (PoC)-Hinweise zu den Schwachstellen herausgegeben haben. Die Veröffentlichung erfolgte, nachdem die Sicherheitsforschenden seit November 2023 mit QNAP bezüglich

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

des o.g. Sachverhalts im vertraulichen Austausch waren. Grund dafür waren Beobachtungen von Unit42, die das Team im Rahmen eines IT-Sicherheitsvorfalls gemacht hatte.

Betroffen von CVE-2023-50358 und CVE-2023-47218 sind folgende QNAP Betriebssystemversionen:

- QTS 4.3.x
- QTS 4.2.x
- QuTScloud c5.x

sowie ältere Versionen von:

- QTS 5.1.x
- QTS 5.0.1
- QTS 5.0.0
- QTS 4.5.x, 4,4,x
- QuTS hero h5.1.x
- QuTS hero h5.0.1
- QuTS hero h5.0.0
- QuTS hero h4.x

Eine vollständige Liste der jeweils betroffenen Softwareversionen findet sich im Advisory [QNAP24].

Bewertung

NAS-Lösungen erfreuen sich sowohl im geschäftlichen als auch im privaten Umfeld aufgrund ihrer vergleichsweise simplen Installation und Bedienbarkeit großer Beliebtheit. Fehlende Sensibilisierung für IT-Sicherheit, mangelndes Patchmanagement oder fehlerhafte Konfigurationen führen jedoch häufig dazu, dass veraltete Systeme aus dem Internet erreichbar sind und zum Ziel von Cyber-Angriffen werden. Auch die ursprünglich von Unit42 gemachten Beobachtungen bestätigen dies.

Die nun erfolgte PoC-Veröffentlichung dürfte in Verbindung mit den zahlreichen, aus dem Internet direkt erreichbaren (veralteten) QNAP-Lösungen dazu führen, dass zeitnah weitere Angriffe stattfinden.

Die genannten Einflussfaktoren erfordern gleichzeitig eine kritische Betrachtung des CVSS-Scores: Wie schwerwiegend die aufgedeckten Sicherheitslücken tatsächlich sind, hängt vom Einsatzzweck und der Umgebung ab, sodass ein mittlerer CVSS-Score der realen Kritikalität des Sachverhalts möglicherweise nicht gerecht wird.

Maßnahmen

IT-Sicherheitsverantwortliche sollten prüfen, ob eine der im Advisory [QNAP2024] angegebenen betroffenen Produktversionen eingesetzt wird, um – wenn nötig – auf eines der vollständig behebenden Releases zu aktualisieren:

- QTS 5.1.5.2645 build 20240116 oder höher
- QTS 5.1.5.2645 build 20240116 oder höher
- QTS 5.1.5.2645 build 20240116 oder höher
- QTS 4.5.4.2627 build 20231225 oder höher
- QTS 4.3.6.2665 build 20240131 oder höher
- QTS 4.3.4.2675 build 20240131 oder höher
- QTS 4.3.3.2644 build 20240131 oder höher
- QTS 4.2.6 build 20240131 oder höher
- QuTS hero h5.1.5.2647 build 20240118 oder höher
- QuTS hero h5.1.5.2647 build 20240118 oder höher
- QuTS hero h5.1.5.2647 build 20240118 oder höher
- QuTS hero h4.5.4.2626 build 20231225 oder höher
- QuTScloud c5.1.5.2651 oder höher

Einige Produktversionen sind bereits seit längerer Zeit nicht mehr von den nun veröffentlichten Schwachstellen (CVE-2023-50358 und CVE-2023-47218) betroffen. Eine genaue Auflistung dazu findet sich im Advisory. Auch wenn

betriebene Systeme mit älteren Software-Versionen vor den hier beschriebenen Sicherheitslücken nur noch während des Installationsprozesses verwundbar sind, muss zum vollständigen Beheben der Sicherheitslücken auf eine der o.g. Versionen aktualisiert werden. [QNAP2024]

Es ist möglich die Verwundbarkeit des Systems zu überprüfen, indem folgende URL aufgerufen wird:

https://<NAS IP>:<NAS system port>/cgi-bin/quick/quick.cgi

Sollte eine HTTP 404 Fehlerseite, wie: "Page not found or the web server is currently unavailable. Please contact the website administrator for help." zurückgeliefert werden, so ist das System nicht betroffen.

Wird eine leere Seite (mit HTTP 200) zurückgeliefert, so ist das System verwundbar und muss aktualisiert werden. Prüfen Sie anschließend erneut die Verwundbarkeit, um sicherzustellen, dass das Update korrekt eingespielt wurde.

Das BSI empfiehlt für exponierte Systeme Sicherheitsupdates grundsätzlich so schnell wie möglich zu installieren und gegebenenfalls verfügbare Auto-Update Funktionalität zu nutzen, sofern ausreichende Backup-Maßnahmen gewährleistet sind. Mehr dazu findet sich im IT-Grundschutzbaustein OPS.1.1.3 [BSI2021].

Links

[QNAP2024] Multiple Vulnerabilities in QTS, QuTS hero and QuTScloud:
https://www.qnap.com/en/security-advisory/qsa-23-57

[UNIT2024] New Vulnerability in QNAP QTS Firmware: CVE-2023-50358:
https://unit42.paloaltonetworks.com/qnap-qts-firmware-cve-2023-50358/

[BSI2024] QNAP NAS: Mehrere Schwachstellen ermöglichen Codeausführung:
https://wid.cert-bund.de/portal/wid/securityadvisory?name=WID-SEC-2024-0353

[BSI2021] OPS.1.1.3: Patch- und Änderungsmanagement (Edition 2021)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2021

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**
  Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

- **TLP:GREEN: Organisationsübergreifende Weitergabe**
  Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
  Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

    TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
    Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

- **TLP:RED: Persönlich, nur für benannte Empfänger**
  Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.