viprinet®

RuggedVPN Stable Firmware Release 10. Oktober 2018 - Version 2018091860/2018100300

Diese Firmware-Version bringt eine Reihe von Verbesserungen der Produktqualität sowie kritische Stabilitätskorrekturen für VPN-Hubs. Wir empfehlen allen Kunden, zeitnah auf diese Version zu aktualisieren.

Ein aktualisiertes Firmware-Image wird auf Amazon AWS verfügbar sein, sobald der AWS Genehmigungsprozess abgeschlossen ist.

Wenn Sie von einer Classic-Firmware upgraden möchten, aktualisieren Sie bitte zuerst den Router auf die letzte stabile Classic-Firmware-Version (Version 2015081830/2015102900 vom 27. November 2015). Bitte berücksichtigen Sie, dass für die Aktualisierung Ihrer Firmware von Classic auf RuggedVPN eine Viprinet Lifetime Maintenance Lizenz erforderlich ist. Weitere Informationen finden Sie unter https://www.viprinet.com/vlm. Es ist möglich, Router und Hubs auf der neuesten Version der Classic-Firmware mit einem Gerät mit RuggedVPN-Firmware zu verbinden. In diesem Fall wird jedoch ein Kompatibilitätsmodus verwendet, der die Leistung und den Funktionsumfang einschränkt. Es wird daher nicht empfohlen ein solches Setup dauerhaft produktiv zu verwenden, ein Classic Firmware Gerät kann jedoch mit einem RuggedVPN Firmware Gerät verbunden sein, während Sie diese Geräte aktualisieren. Der Software VPN Client ist sowohl auf Basis der Classic Firmware als auch alternativ auf Basis der RuggedVPN Firmware Generation erhältlich. Dies ist die letzte Firmware-Version, die noch Verbindungen zu alten Geräten mit unserer Classic-Firmware-Generation (2015 und älter) sowie einem Upgrade von einer solchen Firmware-Version unterstützt.

Folgend eine Auflistung aller neuen Funktionen und Bugfixes im Vergleich zur vorherigen stabilen RuggedVPN Firmware Version (Version 201805236/2018070900 vom 12. Juli 2018):

Fehlerbehebungen

- In der stabilen Version 2018070900 hatten wir die zukünftige Unterstützung für die Weboberfläche vorbereitet, um Unicode (zur Lokalisierung) nutzen zu können. Die Implementierung enthält einen Fehler, der dazu führt, dass der Hub/Router neu gestartet wird, ohne eine Meldung zu geben, wenn ein bestimmtes URL-Format in einer HTTP/HTTPS-Anfrage angegeben wird.

  Leider wird dieser Fehler durch automatisierte Exploit-Scans ausgelöst, die nach Schwachstellen in Webanwendungen suchen. Das bedeutet, dass jedes Viprinet Gerät, dessen Webinterface von dem Internet aus erreichbar ist (was in Ordnung und zu erwarten ist), ohne dass es durch eine ACL geschützt ist, betroffen sein wird. Dies ist ein sehr kritischer Fehler ist. Dieses Update behebt dieses Problem und macht den beteiligten Code wesentlich robuster.

- In einigen seltenen Fällen könnte die Aktualisierung eines 51x-Routers auf die stabile Version 2018070900 dazu führen, dass er während des Bootvorgangs hängt. Dieser Fehler ist nicht bei allen Kunden aufgetreten. Wir konnten jedoch bei den Kunden, die Probleme damit hatten, verifzieren das mit der neuen Version dieser Fehler nicht mehr auftritt.

- Mit dem stabilen Release funktionierten die Funktionen "Minimum guaranteed bandwidth/maximum allowed bandwidth" von QoS nicht mehr wie erwartet. Dies ist nun behoben. (Bug-Ticket #1391)

- Für 200/5xx Router wurde mit dem stabilen Release 2018070900 eine Optimierung zum Lesen von Paketen an interne Routerdienste (Webinterface, SSH CLI) eingeführt. Dies wurde nun entfernt, da CPU-Cache-Bugs zu

Paketverlusten und Neuordnung von Paketen beim Zugriff auf Routerdienste führten. Bei unseren Tests haben wir keine signifikanten Auswirkungen auf die Leistung festgestellt.

- Viprinet-Router enthalten einen Verbindungsbegrenzer, der sicherstellt, dass Sie die Dienste des Routers nicht mit einfachen Einzel-IP-DoS-Angriffen überlasten können. Es stellt sicher, dass nur eine bestimmte Anzahl von Verbindungen pro IP pro Dienst aufgebaut werden kann. In der stabilen Version 2018070900 war dies jedoch in zweifacher Hinsicht unvollständig: Für HTTP/HTTPS und SSH wurde das Limit überhaupt nicht durchgesetzt.

  Ein weiterer bereits seit längerem bekannte Fehler wurde behoben: Wenn zu einem Zeitpunkt eine einzelne IP die maximale Verbindungsgrenze für einen Dienst erreicht hätte, würde dieser Dienst abstürzen. Dies war beispielsweise bei der VPN-WAN-Schnittstelle auf Hubs der Fall - wenn es einer einzelnen IP einmal gelang, 100 gleichzeitige HTTPS-Verbindungen zu öffnen (was sehr unwahrscheinlich ist), konnte kein Channel mehr eine Verbindung zum WAN-Port des Hubs herstellen, bis der Hub neu gestartet wurde.

  Beide Fehler sind behoben. Darüber hinaus haben wir die maximale Anzahl der gleichzeitigen Verbindungen von einer einzigen IP für die folgenden Dienste reduziert:

  - Weboberfläche: 25
  - VPN-Kanäle: 25
  - SSH-Verbindungen: 3
    (Jeweils pro IP)

- Der Code, der darüber entschied, wie viele gleichzeitige WAN-Optimiererverbindungen erlaubt sein sollten, basierte auf der Entscheidung, wie viel freier RAM auf einem Router übrig blieb. Es wurde jedoch nicht berücksichtigt, dass RAM, welcher durch den WAN Optimizer bereits selbst alloziiert wird, auch als "frei" gezählt wird. Dies führte dazu, dass ein Router nach längerem Betrieb oder nach vielen WAN-Optimiererverbindungen die maximal zulässigen WAN-Optimiererverbindungen reduzierte, was dazu führte, dass der WAN-Optimizer kaum noch genutzt wurde.
- Die TCP-Option 254, die ursprünglich für Experimente nach RFC3694-Stil gemäß IANA verwendet wurde, sollte nicht verwendet werden, jedoch haben Kunden berichtet, dass sie Geräte in ihrem Netzwerk haben, die diese Option verwenden. Wir erlauben daher diese TCP-Option nun auf Wunsch eines Partners.
- Wenn Sie Channel haben, die ständig neu verbinden, würde dies zu einem kleinen Speicherleck führen, das mit der Zeit groß werden würde, dass sich der Speicher eines Hubs füllt. (Bug-Ticket: #1399: Speicherleck mit neu verbindenden Kanälen).