

Robustel Router'larda Siber Gvenlik İin Alınabilecek nlemler



Giriş

Son yıllarda IoT ve IIoT kapsamında, nesnelerin internete açılmaya başlamasıyla beraber siber saldırılar da hayli artış göstermeye başladı. Belirli bir IP adresinden başlayıp birçok IP adresini tarayarak, internete açık IP'lere ulaşım sağlamaya çalışan programlar yaygınlaşıyor.

Özellikle son dönemde siber korsanların yukarıda bahsedilen programlar vasıtasıyla, örneğin 5.26.149.1 – 5.26.149.254 aralığında, admin/12345, admin/admin ya da olabilecek default parametreleri kullanarak sıklıkla IP'lere ulaşmaya çalıştıklarını gözlemliyoruz. Bu aralıkta yer alan herhangi bir cihaza erişim sağlandığında, bu durum ciddi tehlikeleri beraberinde getiriyor.

Dolayısıyla, müşterilerimizin son dönemde hayli artış gösteren bu saldırılara yönelik siber güvenlik önlemi almalarında büyük fayda görüyoruz. Aksi takdirde routerları kullanan uygulamalarında ciddi güvenlik açıkları ortaya çıkabileceğinin ve önemli kayıplara neden olabileceğinin altını çizmek istiyoruz.

İyi haber, Robustel Router'ların güvenlik ayarlarının kolayca yapılandırarak bu risklerin en aza indirgenebilecek olması. Bu kılavuzumuzda, Robustel router'larda yapılabilecek bu basit siber güvenlik ayarlarını bulabilirsiniz.

1. Kullanıcı Adı / Şifre Değiştirme

The screenshot shows the Robustel web interface. The top navigation bar includes the Robustel logo, a 'Save & Apply' button, and 'Reboot' and 'Logout' links. A yellow warning banner at the top states: 'It is strongly recommended to change the default password.' The left sidebar contains a menu with categories: Status, Interface, Network, VPN, Services, System, and User Management. The 'System' and 'User Management' items are highlighted with red boxes. The main content area is titled 'Super User Settings' and has two tabs: 'Super User' and 'Common User'. The 'Super User' tab is active. The form contains four input fields: 'New Username', 'Old Password', 'New Password', and 'Confirm Password'. Each field has a red box around it and a help icon. At the bottom right of the form, there are 'Submit' and 'Cancel' buttons, both highlighted with red boxes. The footer contains the text: 'Copyright © 2018 Robustel Technologies. All rights reserved.'

System → User Management

New Username : Dilerseniz kullanıcı adını değiştirebilir, dilerseniz admin olarak da bırakabilirsiniz

Old Password : Eski şifre buraya yazılır

New Password : Yeni şifre buraya yazılır

Confirm Password : Yeni şifre buraya tekrar tanımlanır

Ayarlar tamamlandıktan sonra kaydetmek için **Submit**, sonrasında da **Save & Apply** butonuna tıklanmalıdır.

2. Whitelist Tanımlama

robustel

Save & Apply Reboot Logout

It is strongly recommended to change the default password.

Filtering Port Mapping Custom Rules DMZ Status

Status

Interface

Network

Route

Firewall

IP Passthrough

VPN

Services

System

Enable Filtering ON

Default Filtering Policy Accept

Enable Remote SSH Access OFF

Enable Local SSH Access ON

Enable Remote Telnet Access OFF

Enable Local Telnet

Enable Remote HTTP

Enable Local HTTP

Enable Remote HTTPS

Enable Remote Ping R

Enable DOS Def

Enable Remote IP Forwarding ON

Enable Console ON

Filtering

Whitelist Rules

Index 3

Description

Source Address

Submit Close

Whitelist Rules

Index	Description	Source Address
2	test	192.168.0.0/24

Filtering Rules

Index	Source Address	Source Port	Source MAC	Target Address	Target Port	Protocol
-------	----------------	-------------	------------	----------------	-------------	----------

Submit Cancel

Copyright © 2018 Robustel Technologies. All rights reserved.

Network → Firewall → Whitelist Rules

+ ya tıkladıktan sonra, açılan ekranda;

Description : Kurala vereceğiniz isim

Source Adress : Cihaza bağlanabilecek IP adresi/
Subnetmask tanımı

Örnek : Sadece lokalden erişim istenirse,
192.168.0.0/24 gibi bir tanım yapılabilir (Tanım,
Robustel'in lokal IP'sinin 192.168.0.1 olduğu
düşünülerek verilmiştir)

NOT : Kural olarak sadece Dış IP tanımı yapılırsa, cihaza
uzaktan sadece o dış IP'den internete çıkan cihazlar
erişebilir.

Lokal olarak da erişim sağlanması istenirse, bu tanımın
da ayrıca yapılması gerekir.

3. Cihaza Erişim Yöntemlerini Azaltma

The screenshot shows the Robustel web interface with the following structure:

- Header: robustel logo, Save & Apply, Reboot, Logout
- Notification: It is strongly recommended to change the default password.
- Navigation: Filtering, Port Mapping, Custom Rules, DMZ, Status
- Left Menu: Status, Interface, Network (highlighted), Route, Firewall (highlighted), IP Passthrough, VPN, Services, System
- Main Content: ^ General Settings (Enable Filtering: ON/OFF, Default Filtering Policy: Accept), ^ Access Control Settings (highlighted with a red box), ^ Whitelist Rules, ^ Filtering Rules
- Buttons: Submit, Cancel
- Footer: Copyright © 2018 Robustel Technologies. All rights reserved.

Access Control Settings (highlighted):

- Enable Remote SSH Access: ON/OFF (OFF selected)
- Enable Local SSH Access: ON/OFF (OFF selected)
- Enable Remote Telnet Access: ON/OFF (OFF selected)
- Enable Local Telnet Access: ON/OFF (OFF selected)
- Enable Remote HTTP Access: ON/OFF (OFF selected)
- Enable Local HTTP Access: ON/OFF (OFF selected)
- Enable Remote HTTPS Access: ON/OFF (OFF selected)
- Enable Remote Ping Respond: ON/OFF (OFF selected)
- Enable DOS Defending: ON/OFF (OFF selected)
- Enable Remote IP Forwarding: ON/OFF (OFF selected)
- Enable Console: ON/OFF (OFF selected)

Network → Firewall → Access Control Settings

Cihaza erişim için kullanılacak yöntemler burada yer almaktadır.

Güvenliği artırmak için kullanılmayan erişim yöntemlerini daraltmak faydalı olacaktır.

SSH / Telnet / HTTP / HTTPS gibi ulaşım yöntemleri uzak erişim ya da lokal erişim için kısıtlanabilir.

4. HTTP / HTTPS Portlarını Deęiřtirme



robustel

Save & Apply | Reboot | Logout

It is strongly recommended to change the default password.

Web Server | Certificate Management

^ General Settings

HTTP Port 80 ?

HTTPS Port 8080 ?

Services

Web Server

Submit Cancel

Copyright © 2018 Robustel Technologies. All rights reserved.

Services → Web Server

Bir önceki sayfada, sadece uzaktan HTTPS erişimi açık bırakılmıştı.

Bu sekmeden de default olarak 443 olarak gelen HTTPS portu bir başka port numarası ile deęiřtirilebilir.

NOT : Bu ayar yapıldığı takdirde, cihazın web arayüzüne uzak erişim sağlamak için web tarayıcısına – <https://dışIP:HTTPSport> yazılmalıdır.

Örnek : <https://5.26.149.155:8080>