10 Settings to Lock Down your BIG-IP

David Holmes, 2012-25-10

Earlier this year, F5 notified its customers about a severe vulnerability in F5 products. This vulnerability had to do with SSH keys and you may have heard it called “the SSH key issue” and documented as CVE-2012-1493. **The severity of this vulnerability cannot be overstated**. F5 has gone above and beyond its normal process for customer notification but there is evidence that there are still BIG-IP devices with the exposed SSH keys accessible from the internet. There are several options available to reduce your organization’s exposure to this issue. Here are 10 mitigation techniques that you can implement today to secure your F5 infrastructure.

1. **Install the hotfix. Do it. Do it now.** The hotfix is non-invasive and requires little testing since it has no impact on the F5 data processing functionality. It simply edits the authorized key file to remove access for the offending key.

Control Network Access to the F5

2. Audit your BIG-IP management ports and Self-IPs. Of course you should pay special attention to public addresses (non-RFC-1918), but don’t forget that even private addresses can be vulnerable to internal threats such as malware, malicious employees, and rogue wireless access points. By default, Self-IPs have many ports open – lock these down to just the ones that you know you need.

3. If you absolutely need to have routable addresses on your Self-IPs, at least lock down access to the networks that need it. To lock-down SSH and the GUI for a Self-IP from a specific network:

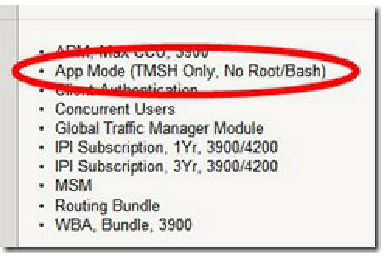
```
(tmos)# modify /sys sshd allow replace-all-with { 192.168.2.* }
(tmos)# modify /sys httpd allow replace-all-with { 192.168.2.* }
(tmos)# save /sys config
```

4. By definition, machines within the network DMZ are at higher risk. If a DMZ machine is compromised, a hacker can use it as a jumping point to penetrate deeper into the network. Use access controls to restrict access to and from the DMZ.

See Solution 13309 for more information about restricting access to the management interface.

Lock down User Access with Appliance Mode

F5’s iHealth system reports consistently that many systems have default passwords for the root and admin accounts and weak passwords for the other users. After controlling access to the management interfaces (see above), this is the most critical part of securing your F5 infrastructure. Here are three easy steps to lock down user access on the BIG-IP.



- APM, Max CCU, 3900
- App Mode (TMSH Only, No Root/Bash)
- Client Authentication
- Concurrent Users
- Global Traffic Manager Module
- IPI Subscription, 1Yr, 3900/4200
- IPI Subscription, 3Yr, 3900/4200
- MSM
- Routing Bundle
- WBA, Bundle, 3900

5. **The Appliance Mode** license option is simple. When enabled, Appliance Mode locks down the **root** user and removes the Unix bash shell as a command-line option– Permitting root login is a historical artifact that many F5 power users cherish. But when root logs in, you don’t know who that user really is, do you? This can be an audit issue if there’s a penetration or other funny business. If you are okay with locking down root but find that you cannot live without bash, then you can split the difference by just setting this db variable to true.

```
(tmos)# modify /sys db systemauth.disablerootlogin value true
(tmos)# save /sys config
```

6. Next, if you haven’t done this already, configure the BIG-IP for remote authentication against, say, the enterprise Active Directory repository. Make this happen from the **System** > **Users** > **Authentication** screen and ensure that the default role is Application Editor or less. You can use the **/auth remote-role command** to provide somewhat granular authorization to each user group.

```
(tmos)# help /auth remote-role
```

7. Ensure that the oft-forgotten ‘admin’ user has no terminal access.

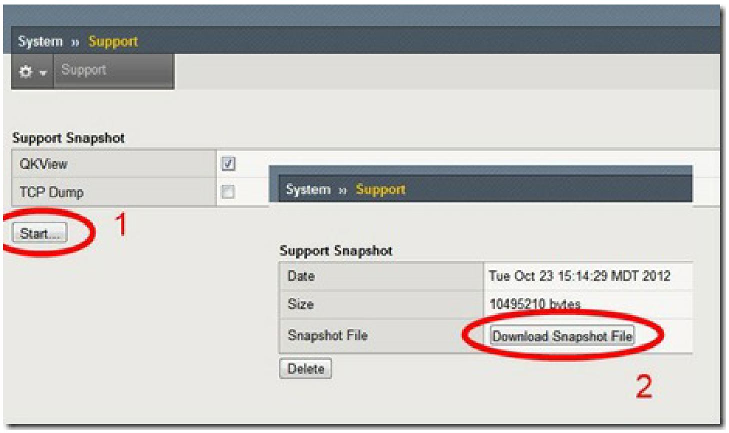
```
(tmos)# modify /sys auth user admin shell none
(tmos)# save /sys config
```

With steps 5-7, you have significantly hardened the BIG-IP device. Neither of the special accounts, root and admin, will be able to login to the shell and that should eliminate both the SSH key issue and the automated brute force risk.

Keep Up to Date on Security News, Hotfixes and Patches

8. If you haven’t done so already, subscribe to the F5 security alert mailing list at f5.com/about-us/preferences. This will ensure that you receive timely security notices.

9. Check your configuration against F5’s heuristic system iHealth. When you upload your diagnostics to iHealth, it will inform you of any missing or suggested security upgrades.



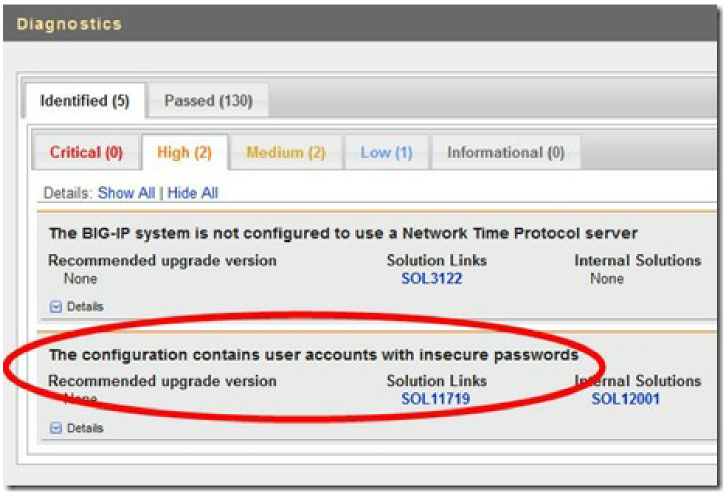
Support Snapshot

QKView ☑
TCP Dump □

Support Snapshot

Date: Tue Oct 23 15:14:29 MDT 2012
Size: 10495210 bytes
Snapshot File: Download Snapshot File

Using iHealth is easy. Generating the support file is as simple as pressing a couple buttons on the GUI. Then point your browser at ihealth.f5.com, login and upload the support file. iHealth will tell you what else to look to help you lock down your system.



The BIG-IP system is not configured to use a Network Time Protocol server

Recommended upgrade version	Solution Links	Internal Solutions
None	SOL3122	None

The configuration contains user accounts with insecure passwords

Recommended upgrade version	Solution Links	Internal Solutions
None	SOL11719	SOL12001

There you have it, nine steps to lock down a BIG-IP and keep on top of infrastructure security… Wait, what, I promised you 10?

10. Follow me (@dholmesf5) and @f5security on Twitter. There that was easy.

If you take anything away from this blog post (and congratulations for getting this far), it is **be sure you install the SSH key hotfix** and protect your management interfaces. And then, fun aside; remember that securing the infrastructure really is serious business.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com