



F5 SLEDFest 2022

Securing and Hardening Your BIG-IP & The importance of keeping your BIG-IP fleet up-to-date

Robin Munley - Engagement Consultant – F5 Professional Services

Device Security Best Practices

F5 Security Hardening Recommendations

F5 Device Security Best Practices

Control Plane touch points and device management access



Authentication and Authorization roles and mechanisms



Device Certificate Configuration

- Management network access and isolation
- Self-IP port lockdown
- Console access
- SSH management access and banners
- HTTPS management access
 - appropriate ACLs -> WebGUI
- SNMP access, community strings, and versioning (v1 / v2c / v3)
- Syslog configuration
- NTP configuration
- DNS configuration
- FIPS / HSM configuration (if required)

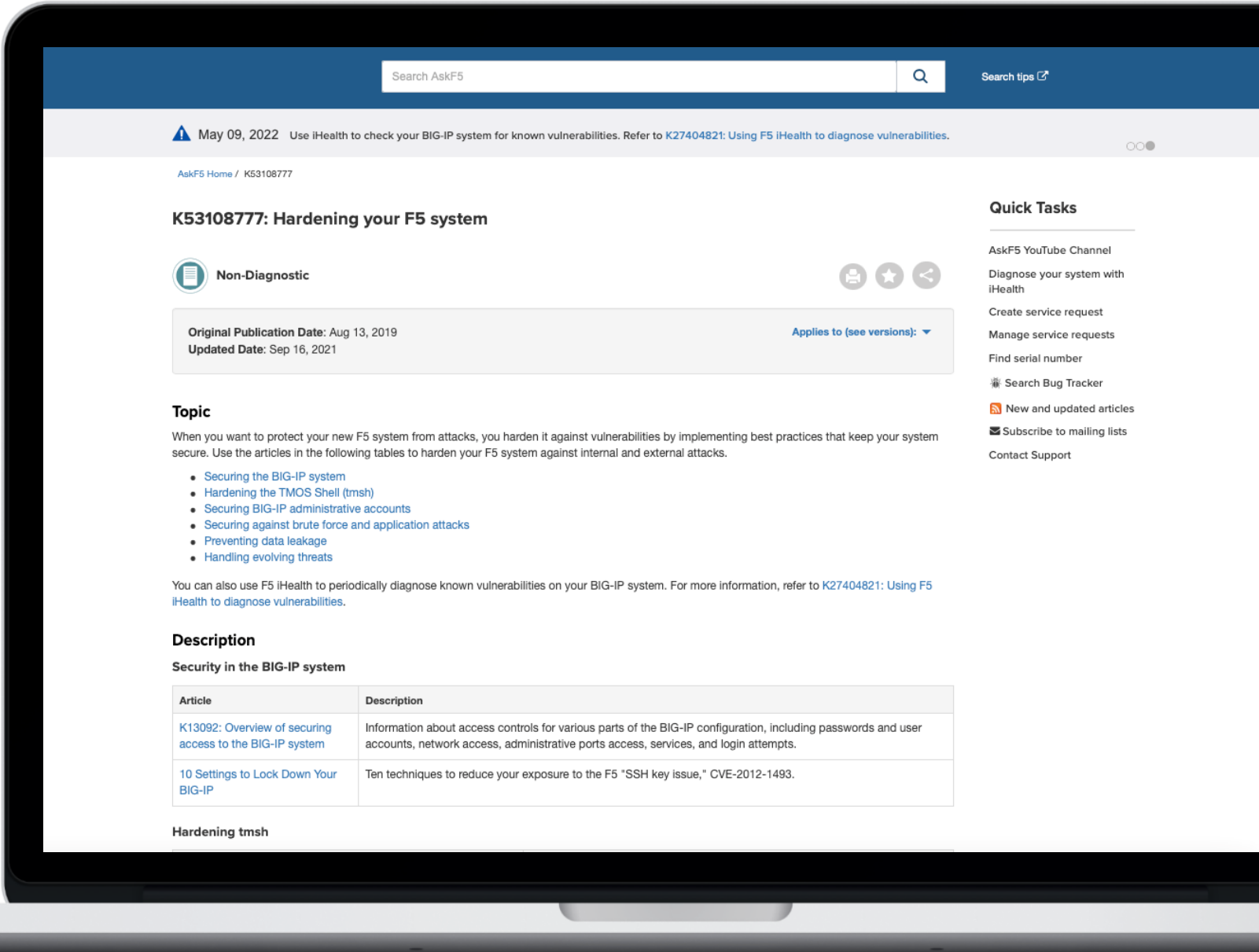
- Setup an external authentication mechanism such a:
 - LDAP / AD
 - TACACS
 - RADIUS
- Sset up the user roles correctly in the external auth systems
- Local accounts
 - Password complexity strategies
 - Password expiry strategies
- Review auditing and alerting functions

- Device certificates must be valid and must not be expired
- Device certificates must be maintained and renewed on each BIG-IP system

K15664

“ When you want to protect your F5 system from attacks, you harden it against vulnerabilities by implementing best practices that keep your system secure.”

K53108777

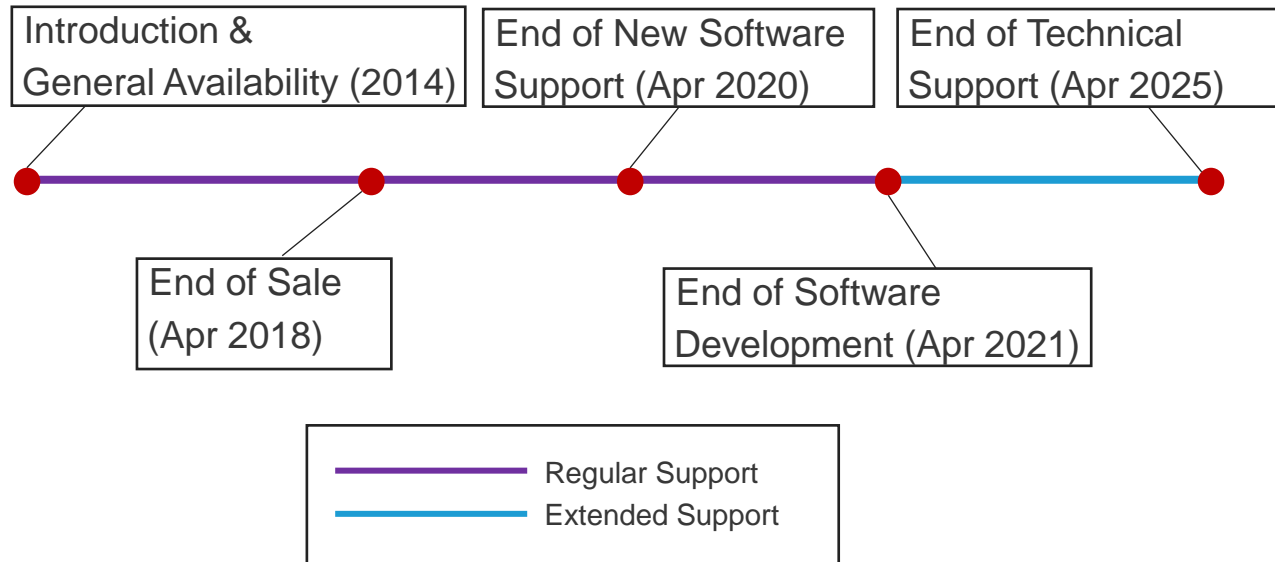


BIG-IP Software Upgrade

Steps to a Successful BIG-IP Upgrade and why you should

BIG-IP Product / Software Lifecycle Overview

EXAMPLE PRODUCT LIFECYCLE



End of Sale (EoS)

- End of sale dates vary by platform; refer to AskF5 for more information.

End of New Software Support (EoNSS)

- New software versions produced after this EoNSS date will not run optimally on the platform due to hardware constraints or minimum system requirements. F5 stops testing whether new software versions produced after this EoNSS date will run properly on platforms designated EoNSS.

End of Software Development (EoSD)

- F5 ceases considering the repair/maintenance of confirmed software/firmware defects for the designated platform or software release. No security patches or code fixes.

End of Technical Support (EoTS)

- F5 ceases to offer technical support for BIG-IP versions that have surpassed their EoTS date

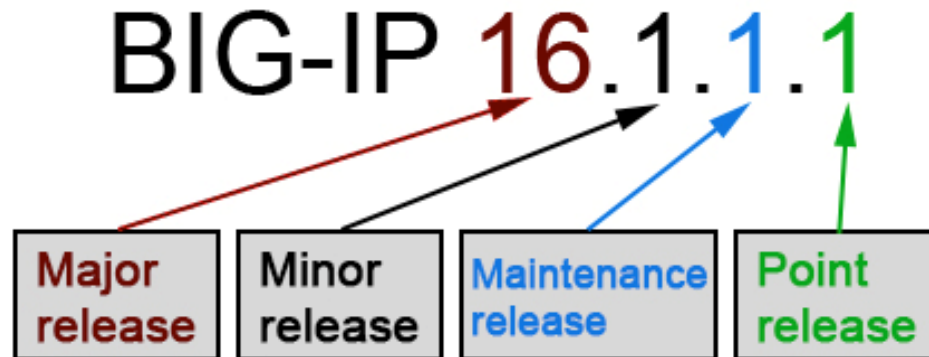
Is It Time For You To Upgrade?

	UPGRADE HIGHLY RECOMMENDED	UPGRADE RECOMMENDED	UPGRADE NOT YET NECESSARY
BIG-IP Versions	v11 & v12	v13 & v14	v15 & v16
Reasons to Upgrade	<ul style="list-style-type: none"> • Access to patches for software bugs or vulnerabilities has expired: <ul style="list-style-type: none"> ○ v11 EoSD – May ‘21 ○ v12 EoSD – May ‘21 • Access to technical support is expiring imminently: <ul style="list-style-type: none"> ○ v11 EoTS – May ‘22 ○ v12 EoTS – May ‘22 • Not leveraging cutting-edge BIG-IP security capabilities • Inability to use innovative new BIG-IP features (e.g. Automation Toolchain, Container Ingress Services) • Newer versions of code inherently more secure 	<ul style="list-style-type: none"> • Access to software patches for bugs or vulnerabilities expiring within 24 months: <ul style="list-style-type: none"> ○ v13 EoSD – Dec ‘22 (<1 year) ○ v14 EoSD – Dec ‘23 • Access to technical support expiring within 24 months: <ul style="list-style-type: none"> ○ v13 EoTS – Dec ‘23 ○ v14 EoTS – Dec ‘23 • Not leveraging cutting-edge BIG-IP security capabilities • Newer versions of code inherently more secure 	<ul style="list-style-type: none"> • None - Great job!

*Specific versions may also be affected by known vulnerabilities as detailed on [Askf5.com](https://www.f5.com/askf5). If you are running one of these versions it's highly recommended that you upgrade.

What is an Update vs. an Upgrade?

Version Schema Definitions



Major release

- Includes significant changes in behavior, added functionality, significant increases in performance, new hardware support, and/or significant architectural changes.

Minor release

- Includes added functionality, increase in performance, new hardware support, and addresses product defects.

Maintenance release

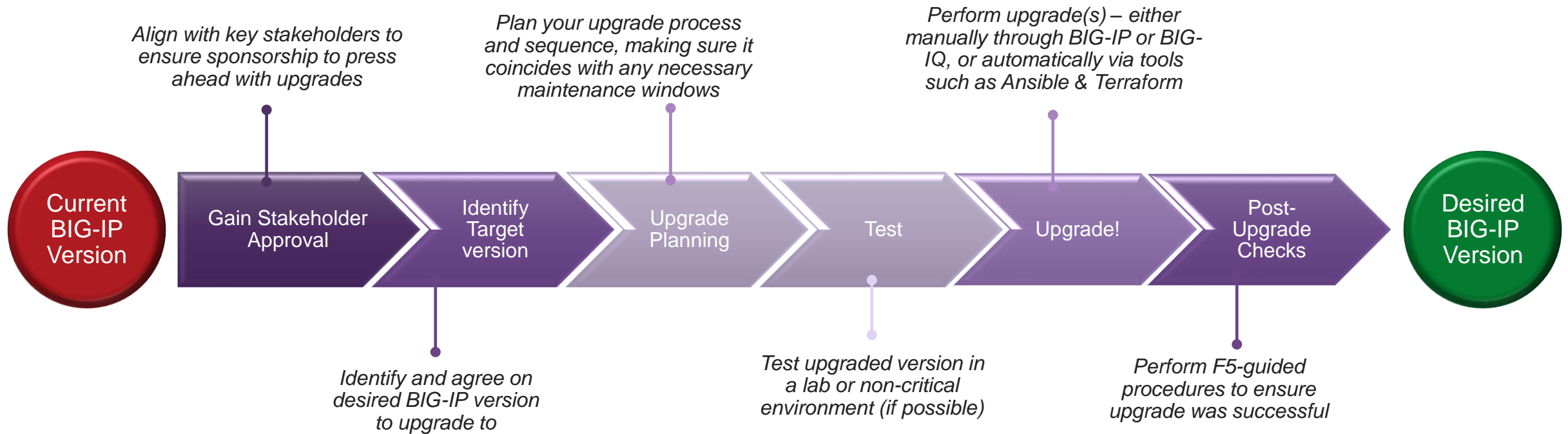
- Contains all previous point releases and addresses additional product defects and security fixes.
- May also contain new diagnostic, supportability improvements, minor functional improvements, and new hardware support; however, will not introduce a change in existing default behavior

Point release

- Is a full release that addresses product defects, including the hardening and refining of existing features and security fixes, and may contain minor functional improvements and new hardware support; however, will not introduce a change in existing default behavior.

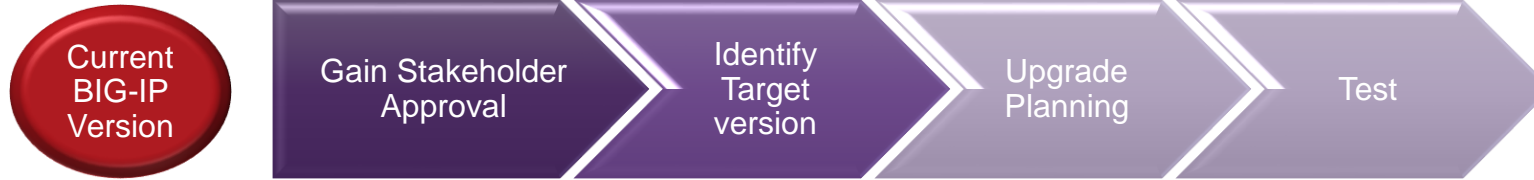
K8986

Steps to a Successful BIG-IP Upgrade



High-level update/upgrade process

Tips while preparing for your update/upgrade



- Change management
- Sync configs for HA pairs
- Proactive Service Request with F5 Support (K16022)
- QKView on ihealth.f5.com (K12878)
- UCS backup and locally download
- Determine the software version/point release you are going to, make sure you [download](#) the updated software and upload the iSO to your BIG-IP platform by using the configuration utility prior to the update window
- Check license activation and reactive your license if you need to
- Verify access to BIG-IP/BIG-IQ
- Baseline service inventory – status of apps
- Grab the master key (f5mku)
- FIPS: Pull your Sys Crypto FIPS file to compare after the update/upgrade
- Do as much testing as possible prior to the update, to ensure full application functionality. If something is not working, do not proceed!

High-level update/upgrade process

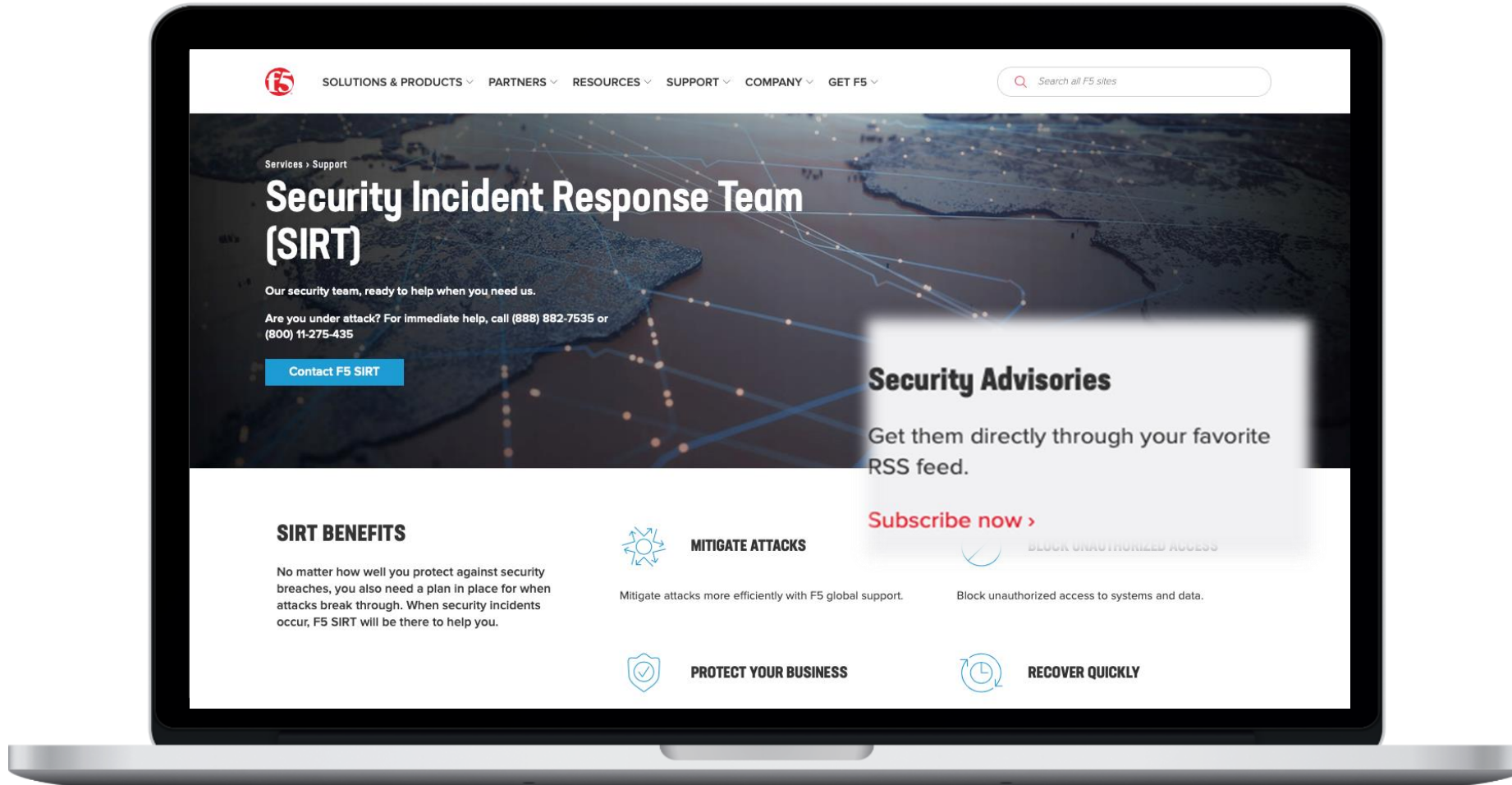
Tips while performing your update/upgrade



- You can use the “[Guide to updating and upgrading BIG-IP](#)”
- [K84554955](#) – Overview of BIG-IP system software upgrades
- Upgrade standby first
- Change your standby to offline to prevent becoming active during reboot
- Reboot to updated version
- Verify status of apps
- Make the updated BIG-IP active
- Repeat for the previously active BIG-IP
- Wrap-up:
 - Verify status of apps and logs
 - QKView to iHealth to check health
 - UCS backup for both BIG-IP

F5 SIRT

How to get notified automatically for security updates



<https://www.f5.com/services/support/security-incident-response-team-sirt>

Subscribing to email notifications

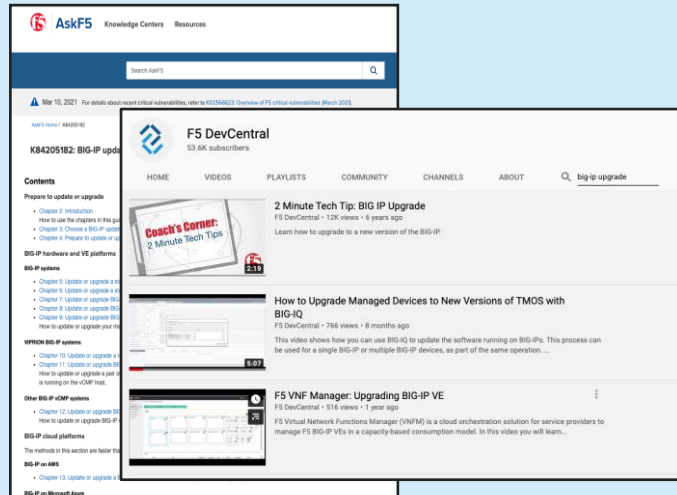
- F5 Security Operations Notifications
- F5 Security Announcements
TechNews Notifications
- TechNews Weekly
- Threat Intelligence Feeds Updates –
Daily
- Threat Intelligence Feeds Updates -
Weekly Wrap-Up

The screenshot shows the AskF5 Knowledge Center interface. At the top, there is a navigation bar with the AskF5 logo, 'Knowledge Centers', and 'Resources'. On the right, there are links for 'Sign Up', 'Sign In', and 'My Support'. Below the navigation bar is a search bar with the text 'Search AskF5' and a magnifying glass icon. A secondary search bar with 'Search tips' is also visible. A notification banner at the top of the content area reads: 'May 26, 2022 F5 has videos to help you upgrade or update your BIG-IP systems. Watch the [Update and upgrade the BIG-IP system playlist](#).' Below this, the breadcrumb 'AskF5 Home / K9970' is shown. The main heading is 'K9970: Subscribing to email notifications regarding F5 products'. To the right of the heading are icons for 'Non-Diagnostic', 'Help', 'Star', and 'Share'. Below the heading, there is a box containing 'Original Publication Date: Sep 18, 2018' and 'Updated Date: Apr 28, 2022', along with a link 'Applies to (see versions):'. The 'Topic' section follows, with a note: 'Note: For information about using an RSS reader to view new and updated documents from F5, refer to K9957: Creating a custom RSS feed to view new and updated documents.' The main text states: 'F5 continuously posts new and updated documents on AskF5. To receive notifications for the most current information, you can subscribe to the following mailing lists, which provide updated information about F5 products and services.' A list of mailing lists is provided:

- **F5 Security Operations Notifications**: Security operations notification for Attack Signature, Fraud Protection Service Signatures/Engine updates, etc.
- **F5 Security Announcements**: Timely alerts about F5 vulnerabilities and high-profile vulnerabilities in third-party components impacting F5.
- **TechNews Notifications**: Brief notifications about special F5 documentation and F5 software releases.
- **TechNews Weekly**: Up-to-date information about F5 software releases, new and updated articles, and new features.
- **Threat Intelligence Feeds Updates - Daily**: Instant notification about new Threat Campaign and Bot signature update releases.
- **Threat Intelligence Feeds Updates - Weekly Wrap-Up**: Weekly notification summarizing Threat Campaigns and Bot signature update releases during that week.

 On the right side of the page, there is a 'Quick Tasks' section with the following items: 'AskF5 YouTube Channel', 'Diagnose your system with iHealth', 'Create service request', 'Manage service requests', 'Find serial number', 'Search Bug Tracker', 'New and updated articles', 'Subscribe to mailing lists', and 'Contact Support'. A large red 'K9970' is overlaid on the bottom right of the screenshot.

Wealth of Resources Available to Support You!



Professional Services

**AskF5 or DevCentral
Website or YouTube**
*Step-by-step upgrade
Documentation and walkthrough*

F5 Support Services
Fast & reliable assistance

F5 Professional Services
*Services that you need
when and how you need them!*

DistiPSSales@F5.com



Thank You!

