disclosure

POWERED BY okta

Hunting CVE-2020-5902

NATE WARFIELD - SECURITY RESEARCHER - @NOX08

whoami

- CTI League Founder #2
- Hacker for 25+ years
- Network engineer for 18 years (10 years @ F5 Networks)
- Network security researcher
- Conference speaker (I miss traveling!)
- https://github.com/n0x08 / @n0x08 on Twitter
- Oh yeah, I'm a Drum&Bass DJ too =)

What exactly is an F5?

- Load Balancer/SSL VPN/ADC/WAF/DNS LB/DPI
- Big expensive network devices which run in most of Fortune 500 (30k+ customers)
  - How expensive? **$30k-$750k**/each (times 2, since they're sold in pairs)
    - Market cap of ~$9B (50% of Citrix)
- CentOS Linux + Apache Tomcat for GUI
- They've had a few nasty vulns over the years....

K13600: SSH vulnerability CVE-2012-1493

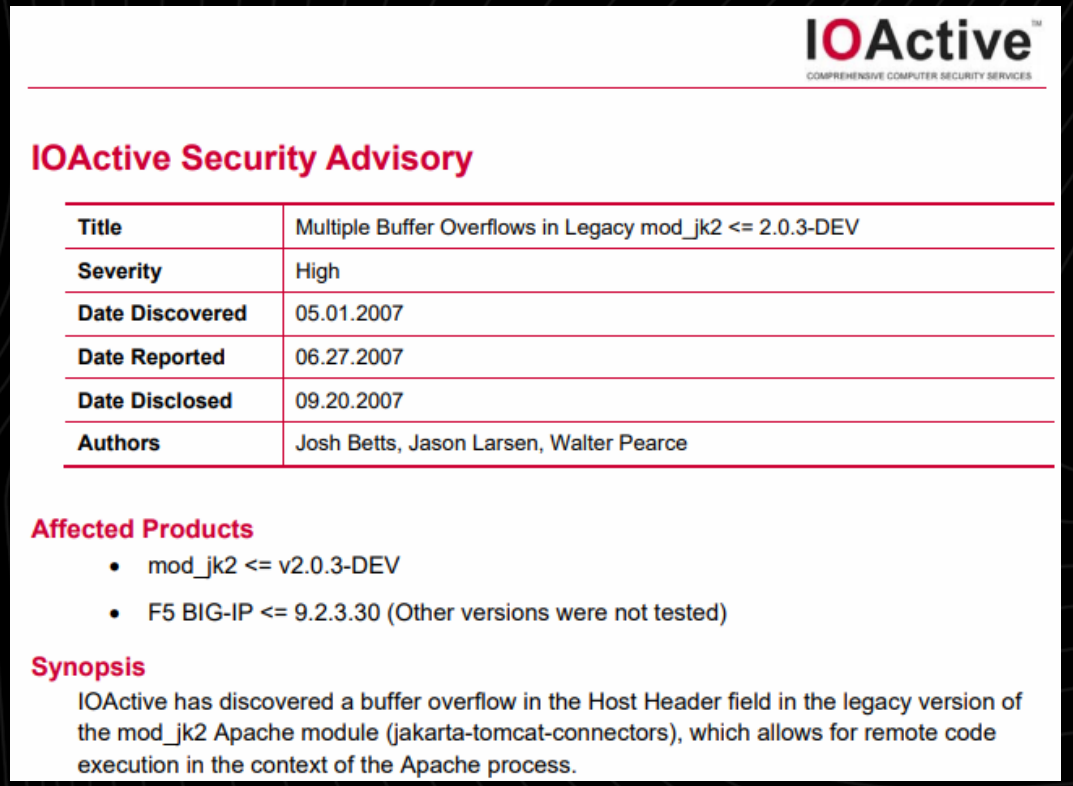
Security Advisory

Original Publication Date: Jun 06, 2012
Updated Date: Jun 18, 2018

Applies to (see versions):

Security Advisory Description

A platform-specific remote access vulnerability has been discovered that may allow a remote user to gain privileged access to affected systems using secure shell (SSH). The vulnerability is caused by a configuration error, and is not the result of an underlying SSH defect.



IOActive
COMPREHENSIVE COMPUTER SECURITY SERVICES

IOActive Security Advisory

Title	Multiple Buffer Overflows in Legacy mod_jk2 <= 2.0.3-DEV
Severity	High
Date Discovered	05.01.2007
Date Reported	06.27.2007
Date Disclosed	09.20.2007
Authors	Josh Betts, Jason Larsen, Walter Pearce

Affected Products

- mod_jk2 <= v2.0.3-DEV
- F5 BIG-IP <= 9.2.3.30 (Other versions were not tested)

Synopsis

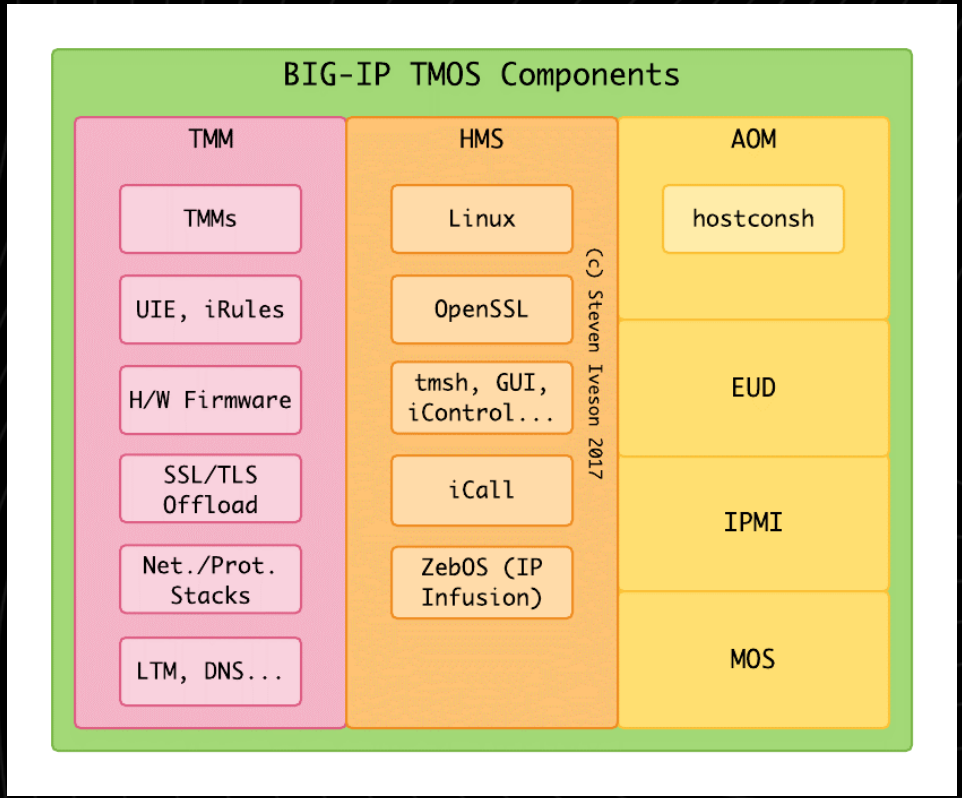
IOActive has discovered a buffer overflow in the Host Header field in the legacy version of the mod_jk2 Apache module (jakarta-tomcat-connectors), which allows for remote code execution in the context of the Apache process.

Why an F5 is a high-value target

- Sits in the core of networks with access to everything.
  - Rarely upgraded due to criticality / poor code quality
- SSL/TLS offloading (certs & keys stored on the device!)
- LDAP/Active Directory/TACACS/RADIUS creds
- VPN session data
- Access to all load-balanced servers
- Modify DNS responses
- They also make great beer taps...

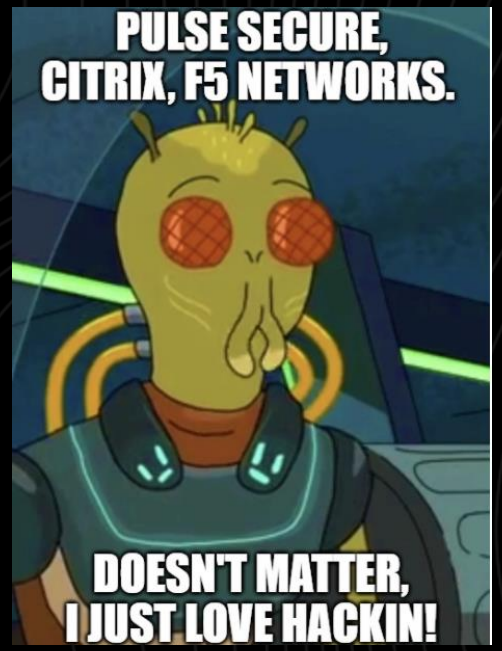
F5 Internal Architecture

- Traffic Management Microkernel (TMM): “Serving Plane” (proprietary)
- CentOS: “Host Management Subsystem”
- No SecureBoot, no firmware validation tools
- No endpoint security
- API: iControl (proprietary)
  - Also a REST version of iControl
- Shells: bash aka “advanced shell”
  - TMSH (proprietary)
  - Also implemented as JSP
  - Zero documentation for JSP version



CVE-2020-5902 – Because security reviews are hard

- *The Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages (K52145254)*
- TL;DR – this is a path traversal vulnerability against the management GUI
- https://$IP/tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=ANYTHING
- F5 does advise against exposing this to the internet
- 10k people didn't follow that advice



F5 approach to patching/mitigation

- Mitigation 1: LocationMatch to block '..;/'
  - Bypassed in ~24 hours
- Mitigation 2: LocationMatch to ALSO block 'hsqldb'
  - This was retracted a day later
  - Un-retracted the following day
- Advance notice to customers? No
- Coordinated patches? No
- IOC tool: 3 weeks after patches

Branch	Versions known to be vulnerable	Fixes introduced in	Severity	CVSSv3 score[1]
16.x	None	16.0.0	Not vulnerable	None
15.x	15.0.0 - 15.1.0	15.1.0.4‡	Critical	10.0
14.x	14.1.0 - 14.1.2	14.1.2.6		
13.x	13.1.0 - 13.1.3	13.1.3.4†		
12.x	12.1.0 - 12.1.5	12.1.5.2		
11.x	11.6.1 - 11.6.5	11.6.5.2		

All TMUI interfaces

Important: This section was last updated on July 8, 2020 at 09:30 Pacific time.

F5 previously provided a configuration-based mitigation for **httpd**, which was intended to block all unauthenticated exploits. Upon further investigation, it has been determined that all previously provided mitigations are not completely effective. F5 continues to investigate; should an effective mitigation be found, this document will be updated with the new information.

F5 recommends installing patched versions of the software to address the underlying vulnerability. The risk may be mitigated by restricting access to all TMUI interfaces via the mitigation steps provided below for self-IPs and the management interface.

15.1.0.4	15.1.0	Release	06/23/2020	15.1.0.4 Release
14.1.2.6	14.1.2	Release	06/10/2020	14.1.2.6 Release
13.1.3.4	13.1.3	Release	06/18/2020	13.1.3.4 Release
12.1.5.2	12.1.5	Release	06/30/2020	12.1.5.2. Release
11.6.5.2	11.6.5	Release	06/17/2020	11.6.5.2 Release

Those who do not learn history are doomed to repeat it

- https://swarm.ptsecurity.com/rce-in-f5-big-ip/
- Mikhail Klyuchnikov also found CVE-2019-19781 (Citrix RCE)!
- *"...take a look at the research "Breaking Parser Logic" by Orange Tsai" (BlackHat 2018)*
- The method he used was disclosed **20 months** before he found the F5 bug
- CVE-2019-19781 was disclosed **5 months** prior
- He didn't find the tmshCmd.jsp POC
- So who did?

Conclusion

We were able to get Remote Command Execution on the F5 Big-IP appliance via the next three easy steps:

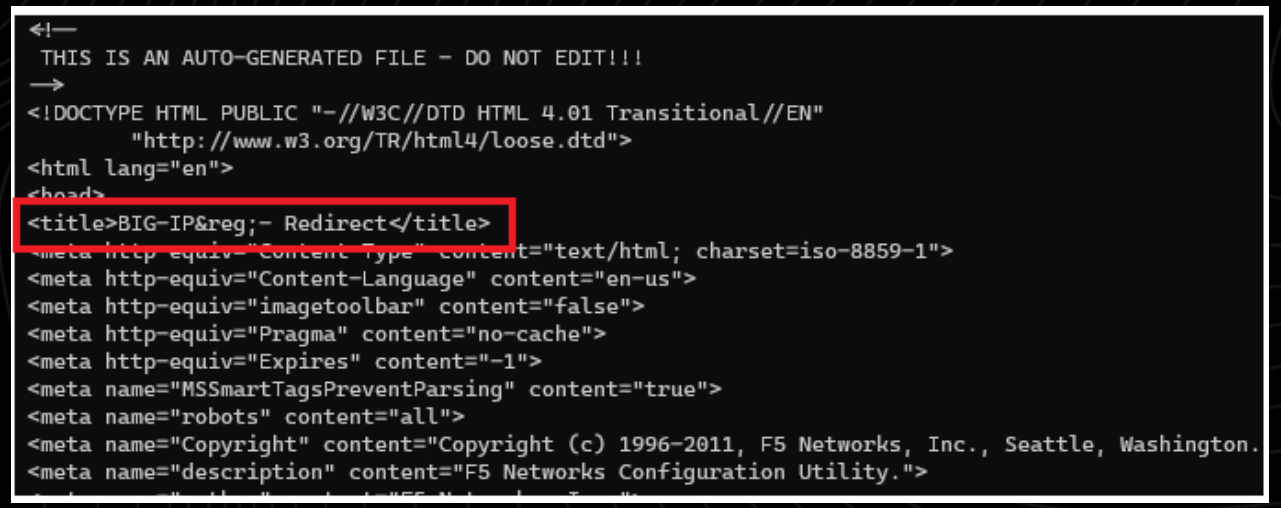
1. Discovering a misconfiguration of the Apache HTTP Server and Apache Tomcat
2. Discovering the use of default credentials for HSQLDB
3. Discovering questionable static methods in the F5 Big-IP TMUI libraries

The timeline:

- 1 April, 2020 — Reported to F5 Networks
- 3 April, 2020 — Vulnerability reproduced by F5
- 1 July , 2020 — Security Advisory and Fixes have been released

CVE-2020-5902 – Hunting techniques

- *"The security firm says it has identified more than 8,000 vulnerable devices that are exposed directly to the internet, including 40% in the United States, 16% in China and 3% in Taiwan."*
- Now, I've been collecting F5 related Shodan dorks for a while....
  - https://github.com/n0x08/ShodanTools
- ....but I didn't have one for their management interface
- Fortunately, a CTI League member had one in his lab
- This was as simple as an 'http.title:' query!
  - https://youtu.be/i7iYcv1XZjA (BHIL 2020)
- 8640 devices exposed (on July 2nd)
- This aligned with the blog 👍

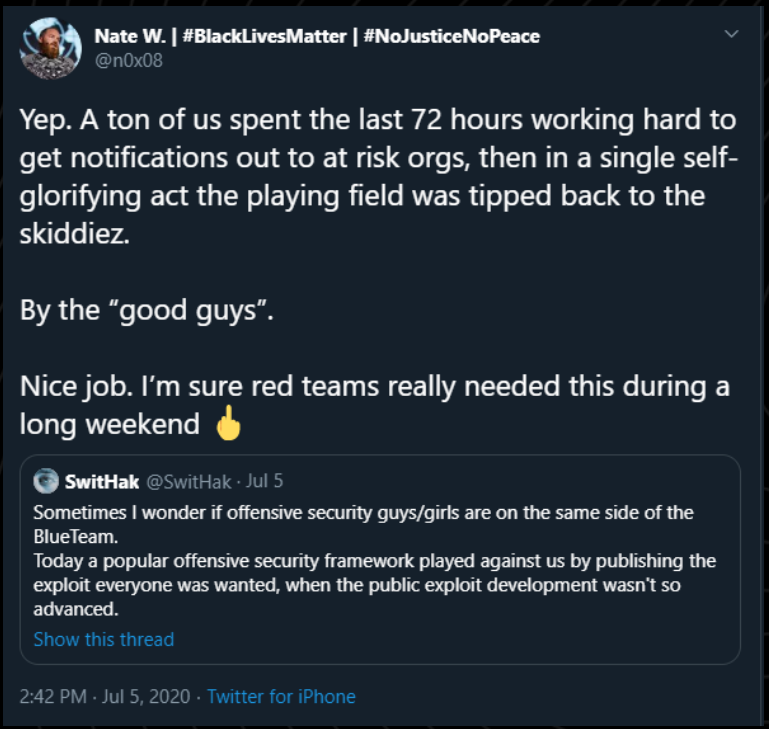


CTI League Response

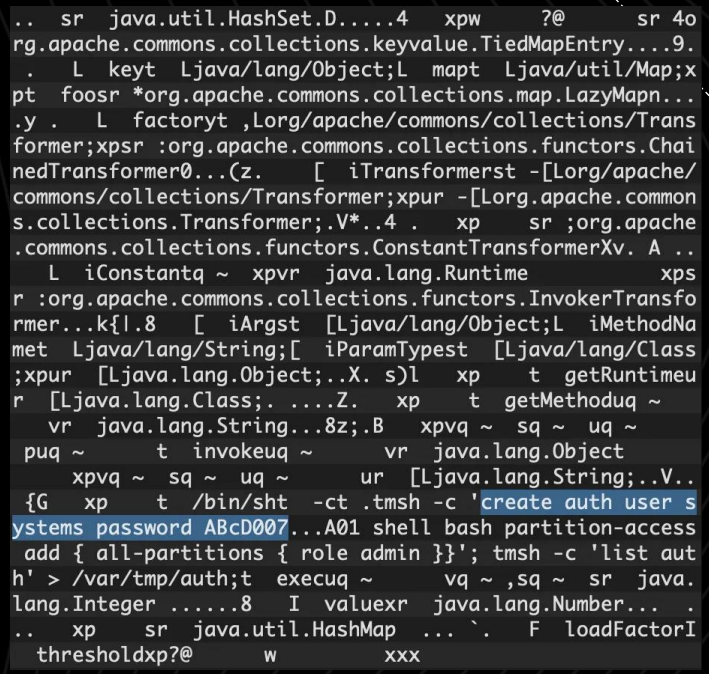
- Downloaded all exposed systems from Shodan
- Parsed out IP/ASN/hostnames/SSL cert details
- Members worked through the 4th of July weekend
- Notified dozens of healthcare orgs, Fortune 500's
- Special thanks:
- @SwitHak, @zero_B_S, Randy Pargman, @emilstahl, Chris F, @mRr3b00t, Eric Brogdon, @tomaszmiklas, David Krause
- Also thanks to the fine folks from @NCCGroupInfosec!

CVE-2020-5902 – Attack timeline

- June 30th – 'K52145254: TMUI RCE vulnerability CVE-2020-5902' published
- July 2nd – CTI League member David Krause & I figured out a Shodan dork
- July 4th – Rich Warren (NCC Group / @buffaloverflow) sees activity in his honeypots
- Rich was kind enough to share the POC with me (good things happen when you ask nicely!)
- July 4th - I send signatures to Shodan & Greynoise
- July 5th – 'someone' drops the POC into a framework
- July 5th – Wide-scale compromise begins
- July 20th – F5 publishes IOC script



CVE-2020-5902 – Two Exploits, One CVE



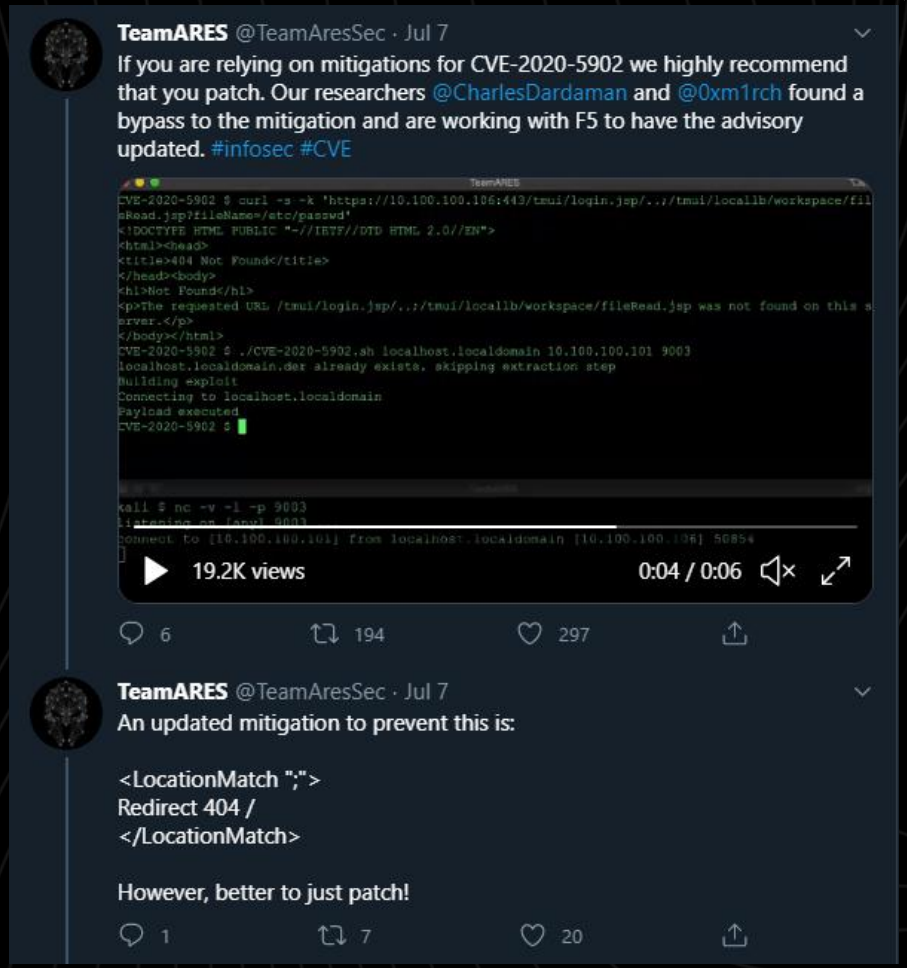
- tmshCmd.jsp - the “second” exploit was the first seen ITW
- Hsqldb – the POC was Java based; this is the “first” exploit
  - ITW exploits seen 2 days AFTER tmshCmd.jsp variant
- Indiscriminate/automated attacks seen in error messages
  - The requested user (bigipuser3) already exists in partition Common.] cmd_data=create auth user bigipuser3 password **** shell bash partition-access add { all-partitions { role admin } }
- IOCs checking via grep string:
  - zgrep -riE '(hsqldb%3b|login.jsp/..%3b/hsqldb|..;/|..%3b/|hsqldb|bigipuser3|systems|run util bash|base64|f5.sh|f5mku|)' /var/log/*
- All of this should have been provided in the advisory

What we found in the rubble

- Web Shells, XMR Miners, PupyRAT & more
- Python port scanners/lateral movement tools
- Indications of advanced knowledge:
  - mount -o {rw|ro},remount /usr; (filesystem workaround)
  - cat /config/bigip/kstore/master (SecureVault device key)
- REST API abused post-compromise once attacker account created
  - Mitigations don't apply to REST; functionality is 'by design' when authenticated
- https://research.nccgroup.com/2020/07/05/rift-f5-networks-k52145254-tmui-rce-vulnerability-cve-2020-5902-intelligence/ - the definitive IOC list

Vulnerability response for mission critical hardware

- Coordinate your patch releases
  - Don’t stagger the fix across 3 weeks of updates
- Fully researched, tested, verified mitigations
  - If it’s not accurate on disclosure day, it’s useless
- IOCs (if known)
  - Don’t have them? Test the POC, provide examples
- Early notification to large customers
  - Use NDAs; this is critical infrastructure!
- InfoSec community != proper response strategy



Closing thoughts

- Security is hard (seriously!)
- Competing vendors are unlikely to learn from each other
- Don’t assume $$$$ == better security
- Black box systems built on OSS have IOT-grade flaws
- Know your network, exposure & risk
- Wear a mask (ACLs)
- Social Distance (network isolation)
- Wash your hands (apply patches)

disclosure

POWERED BY okta

THANK YOU!

NATE WARFIELD - SECURITY RESEARCHER - @NOX08