Critical Citrix Vulnerability

Johannes B. Ullrich Ph.D.
Dean of Research, STI
jullrich@sans.edu

Jason Lam
SANS Certified Instructor
jlam@sans.org

SANS Technology Institute
The best. Made better.

The Vulnerability

- Directory traversal (at least part of it)
- No authentication required
- Can lead to code execution on Citrix Application Delivery Controller / Citrix Gateway
- Easy to exploit (but no public exploit out yet)

Who/What is Affected?

- Citrix ADC / Gateway 13.0
- Citrix ADC / NetScaler Gateway 12.1 / 12.0 / 11.1
- Citrix Netscaler ADC / NetScaler Gateway 10.5

Citrix Suggested Fix

- No actual “patch” released yet
- Instead, Citrix published a workaround
- Workaround blocks access to URLs that contain “/vpns/” or “/../”
- The directory traversal part (‘/../’) only matters if the user (attacker) is connected to the VPN.

Citrix Added Policy

```
add responder action respondwith403 respondwith
   "\"HTTP/1.1 403 Forbidden\r\n\r\n\""


add responder policy ctx267027
   "HTTP.REQ.URL.DECODE_USING_TEXT_MODE.CONTAINS
(\"/vpns/\") && (!CLIENT.SSLVPN.IS_SSLVPN ||
HTTP.REQ.URL.DECODE_USING_TEXT_MODE.CONTAINS
(\"/../\"))" respondwith403 bind responder
global ctx267027 1 END -type REQ_OVERRIDE
```

SANS Technology Institute

Possible False Positives

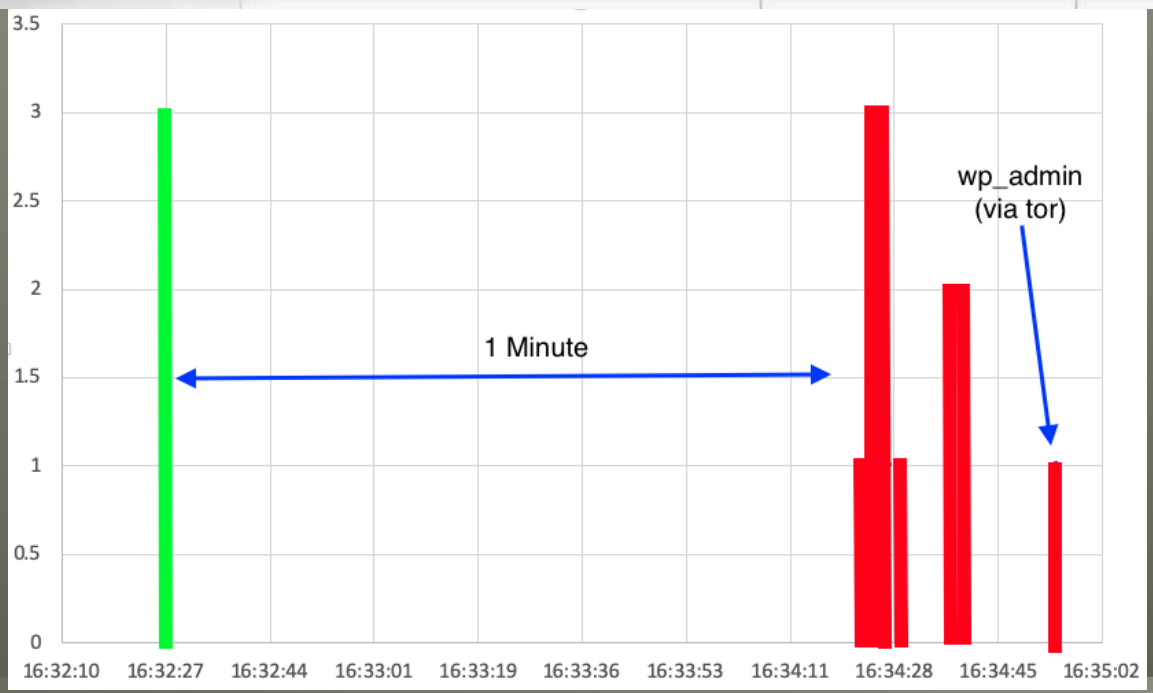
- Application sitting behind a Citrix gateway uses '/vpns/' as part of a URL
- Admin UI links to '/vpns/script/vista/*.exe' for plugins. This will be blocked
- This looks like a simple (too simple?) blacklist.
- Policy may apply to the admin interface as well

How Do Attackers Find Vuln. Systems?

- Shodan/Google/Others… may list some of them
- Certificate Transparency logs
  - Experiment:
    - Configured web server with hostname ‘vpn.*’ or ‘remote.*’
    - Access within minutes after certificate was issued
- Attacker may just scan for files commonly found on server
- Citrix Gateway sets several specific cookies

Certificate Transparency

vpn.	Let's Encrypt Authority X3	5	Dec 28, 2019
citrix	Let's Encrypt Authority X3	1	Dec 27, 2019



SANS Technology Institute

Directory Traversal Vulnerability

```
GET /download.php?file=../../../etc/passwd
```

- Classic input validation flaw
- Impact may be limited if permissions are limited
- Typically associated with information leakage
- But once exploited, can often be leveraged to bypass authentication (reading files with credentials)
- Or can be used to find other vulnerabilities (reading source code)

Fortigate SSLVPN CVE-2018-13379

```
snprintf(s, 0x40, "/migadmin/lang/%s.json",lang)
```

https://example.com/remote/fgt_lang?lang=
/../../../..//////////dev/cmdb/sslvpn_websession

What Did We Find?

- Trivial to upload files to the system without authentication (but filename is somewhat restricted)
- Several directories / files that are writeable by web server and exposed to unauthenticated users
- Missing input validation, and at least in one case, input validation was commented out (debug code left in the release?)

Possible Exploitation (1)

http://example.com/vpns/...
param1=../../../var/www/file.php
param2=<?php exec("rm –rf /")

http://example.com/file.php

Possible Exploitation (1)

http://example.com/vpns/...
param1=../../../var/www/file.php
param2=<?php exec("rm –rf /")

http://example.com/file.php

SANS Technology Institute

Possible Exploitation (1)

Email link

http://example.com/vpns/...
param1=../../../var/www/file.php
param2=<?php exec("rm –rf /")

http://example.com/file.php

SANS Technology Institute

Tactical Mitigations

- Apply the Citrix mitigations
- Consider additional monitoring
  - HTTP requests with /vpns/ and/or /../
  - Citrix ADC, Gateway abnormal traffic towards internal network
  - Do not assume that login will be triggered (it's not required to exploit)
- Layered defense – apply the same blocking and monitoring logic on other inline traffic gateways
- Citrix ADC / Gateway network access review – wide open to internal network?
- Watch for the release of the patch and apply quickly

Thank You!

Questions?

http://isc.sans.edu/slack

Daily Podcasts * Daily ”Diary” Posts * Data Feeds

Twitter: @johullrich / @sans_isc

SANS Technology Institute