Case Study

CVE-2019-11510

Unsolicited vulnerability reporting in practice

Matthijs R. Koot

3 Dec 2019 @ dcypher Symposium 2019

Who am I

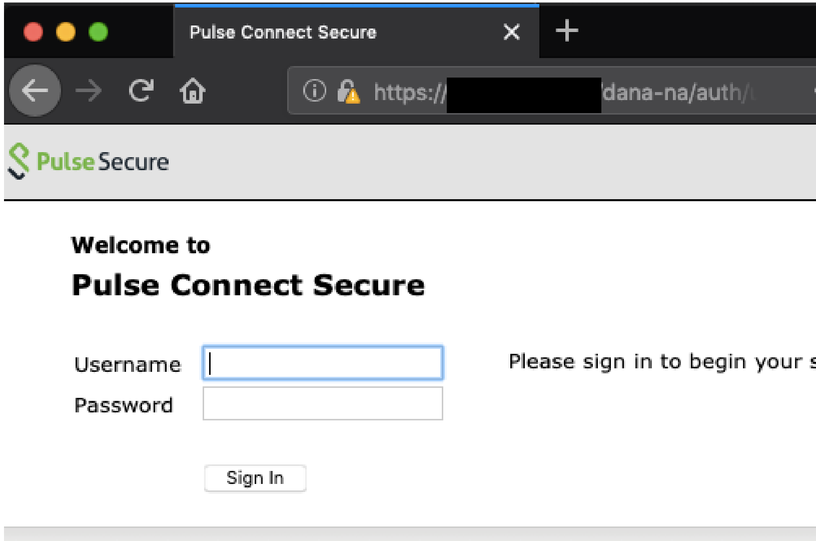
- Twitter: @mrkoot
- Security specialist (7+ years) at Secura
- Research associate at UNIVERSITEIT VAN AMSTERDAM
- Member of NETHERLANDS INTELLIGENCE STUDIES ASSOCIATION NISA

CVE-2019-11510

- Pulse Connect Secure (“PCS”) SSL-VPN
  - Pulse Secure ranked in top 4 “major NAC leaders” in SMB to Large Enterprise (Frost & Sullivan, Oct 2018)
  - 20,000 customers

- CVE-2019-11510 = unauthenticated remote arbitrary file read
  - Discovered by Orange Tsai & Meh Chang
    - March 2019 : reported to vendor
    - April 2019 : vendor released patch (SA44101)
    - August 2019 : presented at BH USA 2019 & Defcon 27
  - In this case: 90s-style path traversal bug (next slide)

- **CRITICAL → CVSSv3 score 10**



Welcome to
Pulse Connect Secure

Please sign in to begin your s

CVE-2019-11510 (cont’d)

- **`GET /dana-na/../dana/html5acc/guacamole/../../../../../..[PATH_TO_FILE]?/dana/html5acc/guacamole/ HTTP/1.1`**

- **Notable values for `[PATH_TO_FILE]:`**
  - **`/data/runtime/mtmp/system`**
    - **Users + hashed passwords**
  - **`/data/runtime/mtmp/lmdb/dataa/data.mdb`**
    - **Cached plaintext passwords**
  - **`/data/runtime/mtmp/lmdb/randomVal/data.mdb`**
    - **Session cookies (`DSID=[...]`) → bypass MFA via session hijacking (!)**

My activities

- August 2019: observed attack payload in my logs

- Obtained list of ~1500 Dutch-registered IPs running PCS
  - Shodan + BinaryEdge
  - did not scan *entire* Dutch IP space myself (this time)

- Tested IPs for CVE-2019-11510
  - Obtained version information
  - Obtained a file w/o user data (= still computer crime?)
    - B/c version information might be unreliable or disputed
  - Enriched IPs w/WHOIS, PTRs and, importantly, hostname(s) in TLS certificate

Results

- 500+ vulnerable systems, many production:
  - Aerospace (flight operators, R&D, [...])
  - Defense industry base (10+ organizations)
  - Chemical industry (a/o petrochemical)
  - Maritime & harbor transport
  - Finance
  - Health (insurer, hospitals, national e-health infra)
  - IT sector (incl. infosec and defense IT contractors)
  - A national government department (i.e., ministry)
  - A few local governments (municipal level)
  - Mainstream media organization
  - [...more...]

What could criminals, state actors or vandals *potentially* gain by compromising these SSL-VPNs?

Hint: A LOT

But... those who were seen dancing are thought to be insane by those who could not hear the music. (Paraphrased from Nietzsche.)

Reporting = PAIN

- Results *immediately* shared w/NCSC-NL
  - Sidenote: NCSC-NL also received report from Bad Packets. Separate effort that globally identified 14,500 (!) vulnerable systems (= how many of the 20,000 customers of Pulse Secure? Unknown.)
- To me as outsider: unclear what happens at NCSC-NL
- 500+ systems, few hundred organizations, **most outside NCSC-NL constituency**
- Hence: contacted organizations myself (=PAIN)
  - Labor-intensive, horrible, thankless work.
  - On top of 40+ hour regular workweek.
  - But stakes are huge... so better keep doing it? ¯_(ツ)_/¯

Reporting = PAIN

- Who do you contact, and how?
  → **KNOWN PROBLEM FOR DECADES, STILL CURRENT. WE SHOULD FIX THIS, BUT HOW?**

- Often: just call general phone number
  - “who are you?”
  - “how do you know this?”
  - “from what company are you?”
  - “is this commercial?”
  - “are you a journalist?”

- Usually not trained to process such calls: no procedure in place (understandably)
- May cause fear within organization
- May expose sensitive info, even if you omit details
- They can’t (and shouldn’t) give out employee contact information to rogue callers

- So: asked to relay message to IT dep’t and/or for callback.

Reporting = PAIN

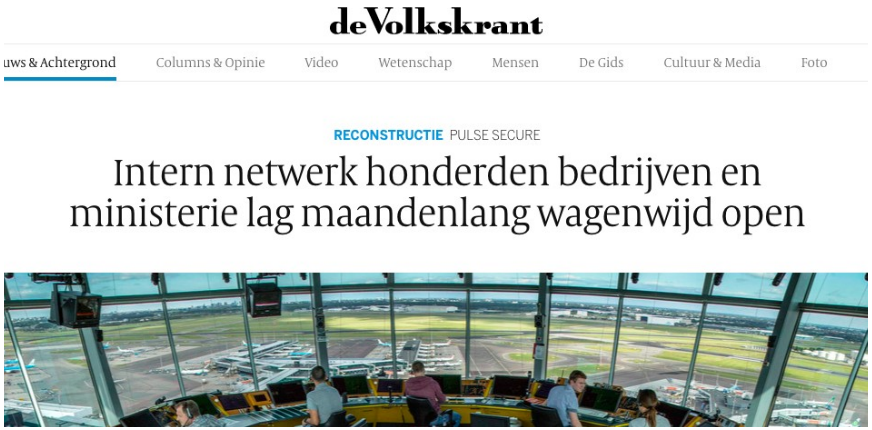
- Recall 5 stages of grief (Kübler-Ross): denial, anger, bargaining, depression, acceptance
- Example responses (N>1):
  - No response
  - “We already patched”
    - ...and yet they’re vulnerable. Some upheld being patched until confronted w/evidence of opposite, then went silent (and patched).
  - “We use MFA”
    - …which can be bypassed via session hijacking. Also: do your users’ creds do not matter to you? Don’t your users use same pass for Gmail etc.?
  - “System is scheduled to be decommissioned”
    - ...but still in use
  - “No longer in production”
    - ...but creds still on system and possibly still current
  - “We’ll fix it in the next patch cycle” (two weeks from now)
    - ...and expose your users/data/systems to pwning for two more weeks?

Reporting = PAIN

- Noticed some important systems (e.g. ABDO) stayed vulnerable
- Turned out NCSC-NL has restrictions on information sharing
  - legal/ethical considerations I was unaware of
- Other Dutch CERTs remained uninformed. Therefore:
- Shared results with o-IRT-o myself
  - Via trusted contact. Not all researchers have this option
- Shared results with Bureau Industrieveiligheid (MIVD) myself
  - Idem

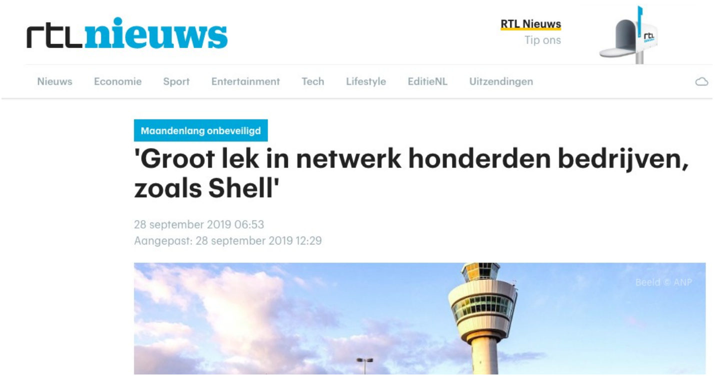
Mainstream media to the rescue?

(last resort... b/c reputations, FUD, waking up sleeping dogs, etc.)



RECONSTRUCTIE PULSE SECURE

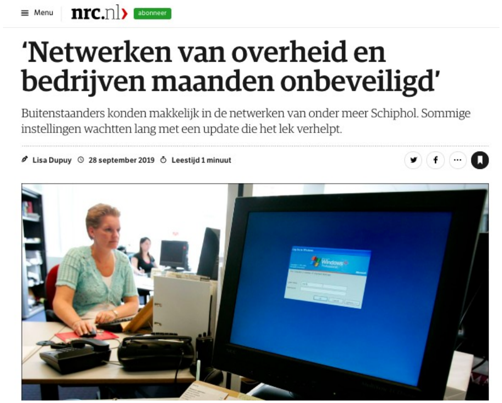
Intern netwerk honderden bedrijven en ministerie lag maandenlang wagenwijd open



Maandenlang onbeveiligd

'Groot lek in netwerk honderden bedrijven, zoals Shell'

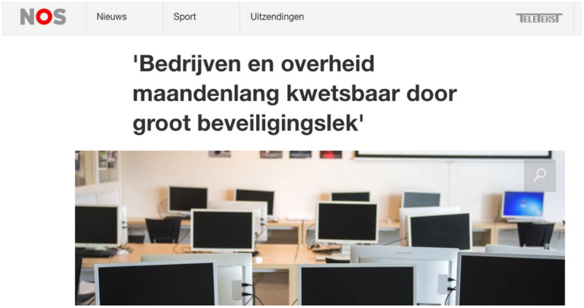
28 september 2019 06:53
Aangepast: 28 september 2019 12:29



'Netwerken van overheid en bedrijven maanden onbeveiligd'

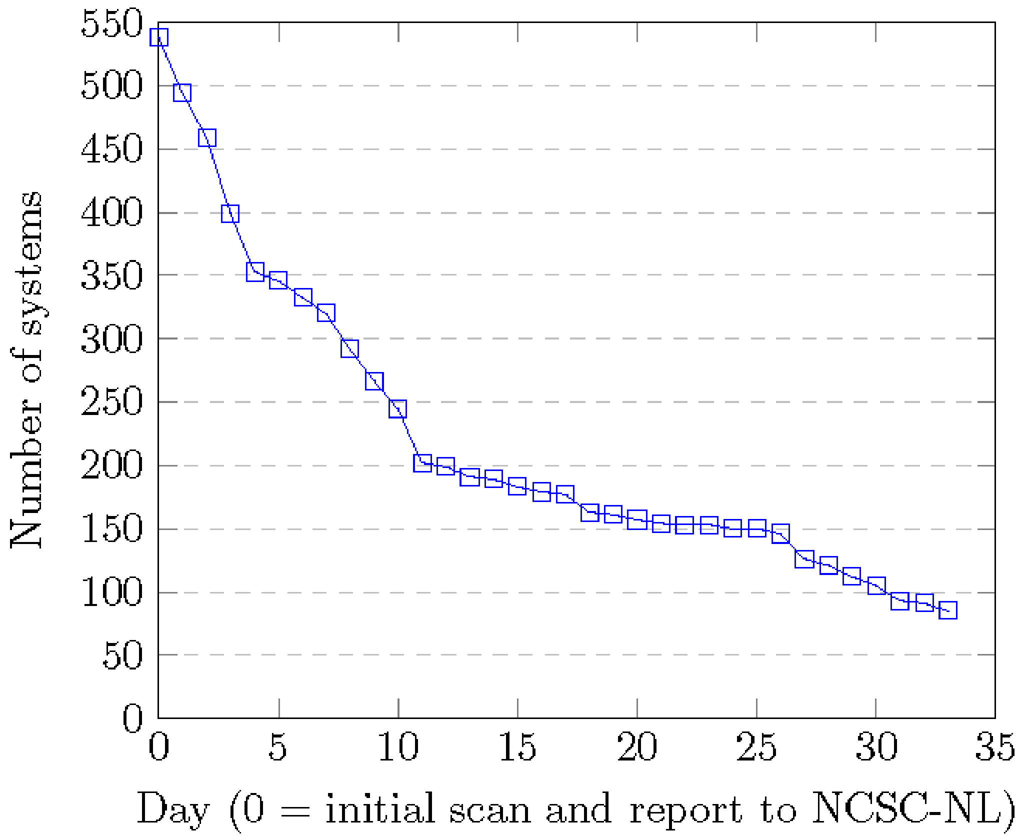
Buitenstaanders konden makkelijk in de netwerken van onder meer Schiphol. Sommige instellingen wachtten lang met een update die het lek verhelpt.

Lisa Dupuy 28 september 2019 Leestijd 1 minuut



'Bedrijven en overheid maandenlang kwetsbaar door groot beveiligingslek'

Progress: patched or offline



Looks good?

Well… be reminded that a single vulnerable production system can pose a serious risk:

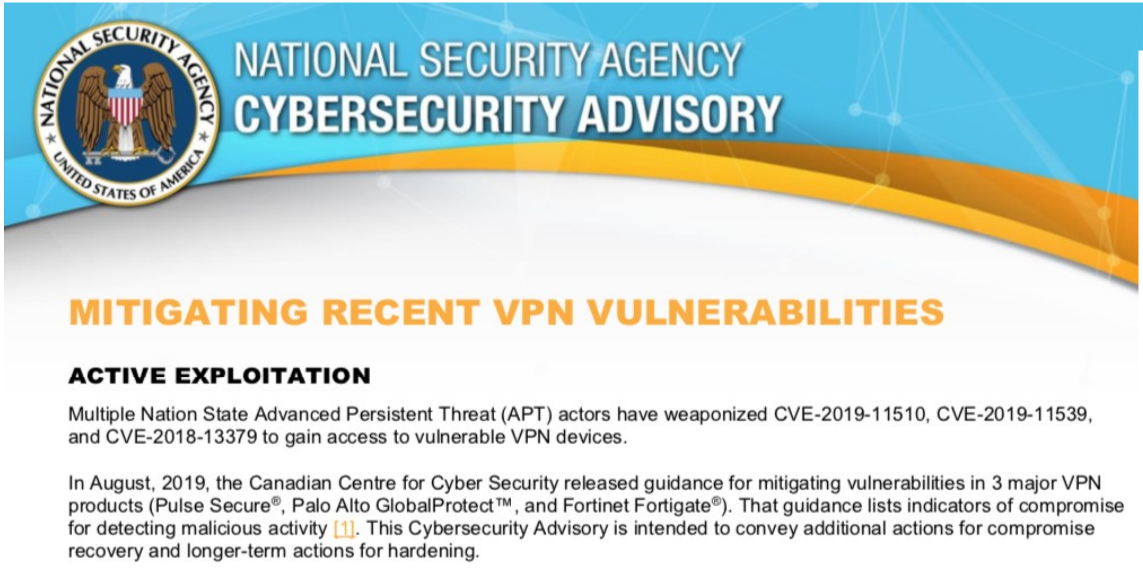
Ransomware: risk to organization

Implants: risk to org + other orgs if used as stepping stone (supply chain attacks)

Data breach: risk to owner + citizens, consumers, patients, etc (= all of us)

Just in time (?)

- October 2019: NSA & GCHQ issue notices that APT actors are exploiting this & other vulns re: Pulse Secure, Fortinet, Palo Alto



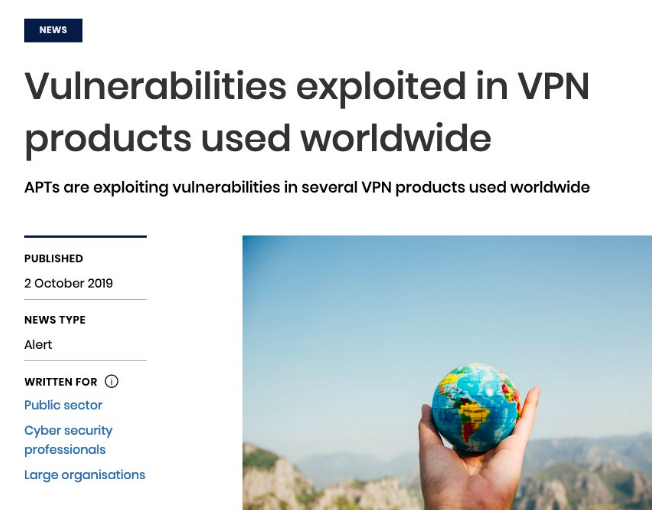
NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

MITIGATING RECENT VPN VULNERABILITIES

ACTIVE EXPLOITATION

Multiple Nation State Advanced Persistent Threat (APT) actors have weaponized CVE-2019-11510, CVE-2019-11539, and CVE-2018-13379 to gain access to vulnerable VPN devices.

In August, 2019, the Canadian Centre for Cyber Security released guidance for mitigating vulnerabilities in 3 major VPN products (Pulse Secure®, Palo Alto GlobalProtect™, and Fortinet Fortigate®). That guidance lists indicators of compromise for detecting malicious activity [1]. This Cybersecurity Advisory is intended to convey additional actions for compromise recovery and longer-term actions for hardening.



NEWS

Vulnerabilities exploited in VPN products used worldwide

APTs are exploiting vulnerabilities in several VPN products used worldwide

PUBLISHED
2 October 2019

NEWS TYPE
Alert

WRITTEN FOR ⓘ
Public sector
Cyber security professionals
Large organisations

Moving forward

- What about the next critical vulnerability that affects internet-facing systems across society?
- **MAKE REPORTING + DISSEMINATION + FOLLOW-UP EASIER**
- DIVD as a new point of contact for unsolicited vulnerability reports
- Improve information sharing
  - within CERT realms
    - PhD candidate working on this: Xander Bouwman / TU Delft
  - to reporters: feedback loop as a form of respect/gratitude?

Moving forward (cont’d)

- **Maybe CERTs should be tasked w/proactively scanning their constituents**? (only for selected high to critical vulns; b/c of autonomy, responsibility, legal aspects, infosec market, etc.)
  - CERTs are close (trusted?) to constituent orgs, often know who to contact.
  - Federated & decentralized scanning to avoid disadvantages of single national system (?)
  - To be coordinated in joint effort that includes NCSC-NL (?)
  - Open questions: opt-in / opt-out, transparency, accountability, etc.
  - Initial idea submitted to o-IRT-o and to ACM DTRAP as part of a Field Note.

- Independent evaluation?
  - Why did so many parties remain vulnerable for four (!) months after vendor issued critical patch?
  - How do 90s-style bugs keep popping up in 2019 even in (internet-facing) security products from long-standing, well-known vendors?
    - Infosec economics, legacy, norms & laws, *bla bla bla*; meanwhile we still have real problems in practice.

Questions?

- Twitter: @mrkoot
- LinkedIn: /in/mrkoot
- Email: koot@cyberwar.nl
- PGP: https://cyberwar.nl/pubkey.asc
  - 51F9 8FC9 C92A 1165