Re: [EXTERNAL EMAIL] - RE: Re: KEV Bypass Report | BOD 22-01

From Intergalactic Auditor <fr0mTheCloud@proton.me>

To Joseph Zadik<jmzadik@fbi.gov>

CC Gatewood, Stanton<stanton.gatewood@cisa.dhs.gov>, Goode, Alisia<alisia.goode@cisa.dhs.gov>

Date Wednesday, February 11th, 2026 at 5:55 PM

10/4 Joe... thank you.

All provided data is Device 1 only (iPhone 14 Pro Max):
- 02.07 KEV Bypass
- 02.08 CoreSight 0x2081 + iCloud exfil

Device 2 telemetry available:
- Additional KEVs bypassed
- India IPsec tunnels (no VPN apps) → Israeli-linked apps (possible SIGINT op)
- 32 live IOCs → telephony C2 infrastructure

Has case ID been assigned for Device 1 packages?

Joseph Goydish II
Atlanta, GA
1(404)-690-3952

On Wednesday, February 11th, 2026 at 5:41 PM, Joseph Zadik <jmzadik@fbi.gov> wrote:

> Hi Joseph,
>
> If there are follow-up questions on the information provided, you will contacted at that time.
>
> Thank you,
> Joe
>
> ---
>
> **From:** Intergalactic Auditor <fr0mTheCloud@proton.me>
> **Sent:** Wednesday, February 11, 2026 2:31:57 PM
> **To:** Zadik, Joseph M. (AT) (FBI) <jmzadik@fbi.gov>
> **Cc:** Gatewood, Stanton <stanton.gatewood@cisa.dhs.gov>; Goode, Alisia <alisia.goode@cisa.dhs.gov>
> **Subject:** Re: [EXTERNAL EMAIL] - RE: Re: KEV Bypass Report | BOD 22-01
>
> Joe/Stanton/Alisia,

UPLOADED "02.08 CVE-2026-25251 EXPLOITATION.zip"
- EXPLOITATION_REPORT.txt + .json
- logdata_LiveData.tracev3
- tracev3_exploitation_analyzer.py
- 8x CoreSight 0x2081 hits (fuses=0, Feb 8 LIVE)
- iCloud Exfil/
  * Network Exfiltration.txt
  * tracev3_network_analyzer.py
  * CloudKit data exfil DURING debug exploitation

GitHub: https://github.com/Str8tdr0p/unblown-fuses-iphone-promo

YES/NO:
1. 02.08 folder + iCloud Exfil examined?
3. GitHub analyzed?
4. UCG needed?

Thank you,
Joseph Goydish II
1(404)-690-3952
On Wednesday, February 11th, 2026 at 11:05 AM, Intergalactic Auditor <fr0mTheCloud@proton.me> wrote:

> Hi Joe and DHS members,
>
> Checking in on the Feb 10 portal ZIP (.tracev3 SHA256 verified) and GitHub repo dropped 12:11am [https://github.com/Str8tdr0p/unblown-fuses-iphone-promo].
>
> Repo contains VINCE VU#132084.1 evidence (CISA-validated TI SN27xxx unfused debug fuses) + repro scripts potentially linking the hardware persistence to KEV exploitation patterns.
>
> The GitHub link also documents MITRE reserving CVE-2026-25251 then refusing publication despite public references… leaving the VINCE-validated hardware persistence untracked in official channels.
>
> Could you confirm:
> 1. Portal submission reviewed?
> 2. GitHub repo/scripts examined?
> 3. Next steps for secure transfer of additional artifacts (Device 2, 32+ IOCs)?
>
> Thank you,
> Joseph Goydish II

-------- Original Message --------
On Wednesday, 02/11/26 at 00:11 Intergalactic Auditor <fr0mTheCloud@proton.me> wrote:

> Coming in hot
>
> https://github.com/Str8tdr0p/unblown-fuses-iphone-promo
>
> -------- Original Message --------
> On Tuesday, 02/10/26 at 19:28 Intergalactic Auditor <fr0mTheCloud@proton.me> wrote:
>
> > [02.07_KEV_Bypass (iOS26.2.1).zip] uploaded to portal.
> >
> > Package Contents:
> >
> > - 02.07-Active-KEV-Bypass.md: Forensic report documenting active exploitation of 3 CISA KEV CVEs (CVE-2025-24200, CVE-2025-43200, CVE-2025-43300) on iPhone 14 Pro Max iOS 26.2.1, POST-PATCH, POST-DFU RESTORE, iCloud-only config.
> >
> > - logdata_LiveData.tracev3: Raw binary log (SHA256: b0a14e4e0f7eaf9b6d741e161864bee61810bf2705470e57991c29eb6e67e7e5)
> >
> > - Parsing script: Reproducible extraction of all offsets/IOCs from trace.
> >
> > Key Network IOCs Documented:
> > - Rogue gateway: 192.168.8.1 (MAC: d8:b3:70:47:77:57), subnet 192.168.8.0/24
> > - C2 Node 1: 20.1.1.7:443 (Microsoft Azure AS8075)
> > - C2 Node 2: 38.1.1.4:443 (Unknown ARIN)
> > - Multicast beacon: 233.1.2.1
> > - Token API: gateway.i[...]:443/ck/base/api/client/asset/retrieve/token
> >
> > Core Finding: "Physically impossible" state device locked + 4x bypassPCS + keychain access + USB pairing + rogue network + encrypted C2... all simultaneous on clean device.
> >
> > Thank you,
> > Joseph Goydish II
> >
> > On Tuesday, February 10th, 2026 at 6:27 PM, Intergalactic Auditor <fr0mTheCloud@proton.me> wrote:
> >
> > > Hey Joe, thanks for the link!
> > >
> > > February 7 forensic package is being uploaded to secure portal (3 KEVs, rogue network, Azure C2) right now.

ADDITIONAL INTELLIGENCE AVAILABLE:

Device 1 (Feb 8-10): 3 additional KEVs, escalating activity, fresh IOCs.

Device 2 (separate): Multi-nation foreign intelligence infrastructure - Israeli services (IDF Unit 8200 investor connections), Taiwan government telecom staging, Japanese proxy, Russian services, blockchain DNS. 32+ actionable IOCs. None of these apps installed.

TRANSFER CONDITION:

Confirmation required: Is this foreign intelligence surveillance (FBI Counterintelligence) or cybercrime (FBI Cyber)?

Infrastructure involves Israeli Unit 8200-connected services, Taiwan government telecommunications, multi-nation coordination. This is targeted surveillance of US persons, not criminal hacking.

I am available to discuss and confirm investigative jurisdiction and evidence handling. Given the foreign intelligence indicators and ongoing exploitation, in-person technical briefing is preferred over the portal transfer.

Thank you,
Joseph Goydish II

On Tuesday, February 10th, 2026 at 5:47 PM, Joseph Zadik <jmzadik@fbi.gov> wrote:

> Good evening Joseph,
>
> Your IC3 was received with the information you provided. You will be receiving a teleporter link, which is secure and encrypted, where you can upload the additional relevant information.
>
> Thank you,
> Joe
>
> ---
>
> **From:** Intergalactic Auditor <fr0mTheCloud@proton.me>
> **Sent:** Tuesday, February 10, 2026 3:20 PM
> **To:** Zadik, Joseph M. (AT) (FBI) <jmzadik@fbi.gov>
> **Cc:** Gatewood, Stanton <stanton.gatewood@cisa.dhs.gov>; Goode, Alisia <alisia.goode@cisa.dhs.gov>
> **Subject:** [EXTERNAL EMAIL] - RE: Re: KEV Bypass Report | BOD 22-01
>
> Hello Joseph,
>
> Please see the attached thread. Can we discuss this further?

Thank you,
Joseph Goydish II
On Tuesday, February 10th, 2026 at 2:59 PM, Gatewood, Stanton <stanton.gatewood@cisa.dhs.gov> wrote:

> Please forward this to Joseph Zadik jmzadik@fbi.gov. Also, include Ailisa Goode, <alisia.goode@cisa.dhs.gov>, as she is the DHS CISA/FBI liaison…
>
> Best
>
> Stanton Gatewood
>
> Cybersecurity State Coordinator
>
> Cybersecurity and Infrastructure Security Agency (CISA)
>
> Integrated Operations Division | Region 4 – Georgia
>
> stanton.gatewood@mail.cisa.dhs.gov
>
> P: [redacted]

From: Intergalactic Auditor <fr0mTheCloud@proton.me>
Sent: Tuesday, February 10, 2026 2:54 PM
To: Gatewood, Stanton <stanton.gatewood@cisa.dhs.gov>
Subject: RE: Re: KEV Bypass Report | BOD 22-01

No sir I have not. And have documented token theft + continued exploitation every day since Friday. As well as enriched infrastructure updates.

On Tuesday, February 10th, 2026 at 2:51 PM, Gatewood, Stanton <stanton.gatewood@cisa.dhs.gov> wrote:

> Have spoken to the FBI yet?
>
> Stanton Gatewood
>
> Cybersecurity State Coordinator
>
> Cybersecurity and Infrastructure Security Agency (CISA)
>
> Integrated Operations Division | Region 4 – Georgia
>
> stanton.gatewood@mail.cisa.dhs.gov
>
> P: [redacted]
>
> 
>
>
> ---
>
> **From:** Intergalactic Auditor <fr0mTheCloud@proton.me>
> **Sent:** Tuesday, February 10, 2026 2:24 PM
> **To:** Gatewood, Stanton <stanton.gatewood@cisa.dhs.gov>
> **Subject:** Fw: Re: KEV Bypass Report | BOD 22-01

Hello Stanton,

I have an ongoing incident that has been escalated by Klint Walker at Region 4. The foreign infrastructure identified is exploiting CVEs listed in the KEV, but is doing so on fully patched devices.

Below is a summary of what has taken place and where the bottleneck sits. Is there a way you can guide me in the best path forward?

Thank you.
Joseph Goydish II

------- Forwarded Message -------
From: Intergalactic Auditor <fr0mTheCloud@proton.me>
Date: On Saturday, February 7th, 2026 at 6:06 PM
Subject: Re: KEV Bypass Report | BOD 22-01
To: Walker, Klint <klint.walker@cisa.dhs.gov>
CC: Goode, Alisia <alisia.goode@cisa.dhs.gov>

> Klint/Alisia,
>
> Klint/Alisia, noting for documentation that we've passed the 24-hour mark since the Friday handoff. To ensure alignment with **AG Guidelines Art. IV**, **FBI Directive 1355D**, and **6 U.S.C. § 681a**, I am flagging this FBI intake delay. Please advise on the status of establishing the secure channel for the 2nd device artifacts.
>
> Thank you,
> Joseph Goydish II
>
> On Saturday, February 7th, 2026 at 9:33 AM, Intergalactic Auditor <fr0mTheCloud@proton.me> wrote:
>
> > 3 additional KEV listed CVE's found exploited in that 2nd device referenced.
> >
> > CVE-2023-41064
> > CVE-2025-43529
> > CVE-2025-24085

Summary of the attack is attached to this email.

I will hold off on further drops until we can assure secure comms.

Thank you

On Friday, February 6th, 2026 at 11:13 PM, Intergalactic Auditor <fr0mTheCloud@proton.me> wrote:

> No sir not yet.
>
> From the same dump:

Domain	Frequency	Geopolitical Context	Forensic Logic / 1320 Significance
le.com	**74x**	**China** (LeEco/Tech Stack)	**Persistent Telemetry Inundation.** High-volume heartbeat masking data exfiltration via Chinese tech infrastructure.
yandex.net	**1x**	**Russia** (Kremlin-controlled)	**Forensic "Ghost" Beacon.** A single-hit verification handshake/witness from the primary Russian indexing core.

On Friday, February 6th, 2026 at 11:04 PM, Walker, Klint <klint.walker@cisa.dhs.gov> wrote:

> Mi will send up again. Has anyone reached out to you at this time ?

From: Intergalactic Auditor <fr0mTheCloud@proton.me>
Sent: Friday, February 6, 2026 11:00:59 PM
To: Walker, Klint <klint.walker@cisa.dhs.gov>
Cc: Goode, Alisia <alisia.goode@cisa.dhs.gov>
Subject: Re: KEV Bypass Report | BOD 22-01

Apologies for the late night follow up, but my ethics won't allow me to sit on these.

Especially given the Friday night tactical window in which they just appeared....
(extracted from a second device showing similar KEV exploitation patterns)

IP Address	File Source (.tracev3)	ISP / ASN Context	Fu
27.1.1.33	`00000000000005a9.tracev3`	**China Unicom** (AS9800)	`3f`
39.1.1.32	`00000000000005a9.tracev3`	**China Telecom** (AS4812)	`3f`
49.1.1.1	`00000000000005b1.tracev3`	**Thailand/SE Asia**	`a1`

On Friday, February 6th, 2026 at 8:04 PM, Intergalactic Auditor <fr0mTheCloud@proton.me> wrote:

> Thanks Klint,

Being able to add context to all of this should produce actionable intel.

-------- Original Message --------
On Friday, 02/06/26 at 16:59 Walker, Klint <klint.walker@cisa.dhs.gov> wrote:

> Alisia,
>
> Can you introduce Joseph to our local cyber FBI team to coordinate? Thank you.
>
> ---
>
> **From:** Intergalactic Auditor <fr0mTheCloud@proton.me>
> **Sent:** Friday, February 6, 2026 4:16:06 PM
> **To:** Walker, Klint <klint.walker@cisa.dhs.gov>
> **Subject:** KEV Bypass Report | BOD 22-01
>
> **CAUTION:** This email originated from outside of CISA/DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.
>
> Hello Klint,
>
> Thanks for taking the call. Attached are 2 reports highlighting the active exploitation of 3 KEV listed CVEs. The raw artifact and parsing scripts are available per request.
>
> CVE-2025-24200
> CVE-2025-43200
> CVE 2025-43300
>
> Thank you,
> Joseph II

20.47 KB 1 embedded image

image001.png 20.47 KB