Hacker Leaks 8.5M U.S. Environmental Protection Agency (EPA) Contact Data (UPDATED)

Published: 2024-04-07 · Archived: 2026-04-05 14:26:02 UTC

The U.S. Environmental Protection Agency (EPA) is experiencing a major data leak incident involving a known hacker using the alias USDoD. This issue involves a third-party company and affects over 8.5 million users and businesses around the world.

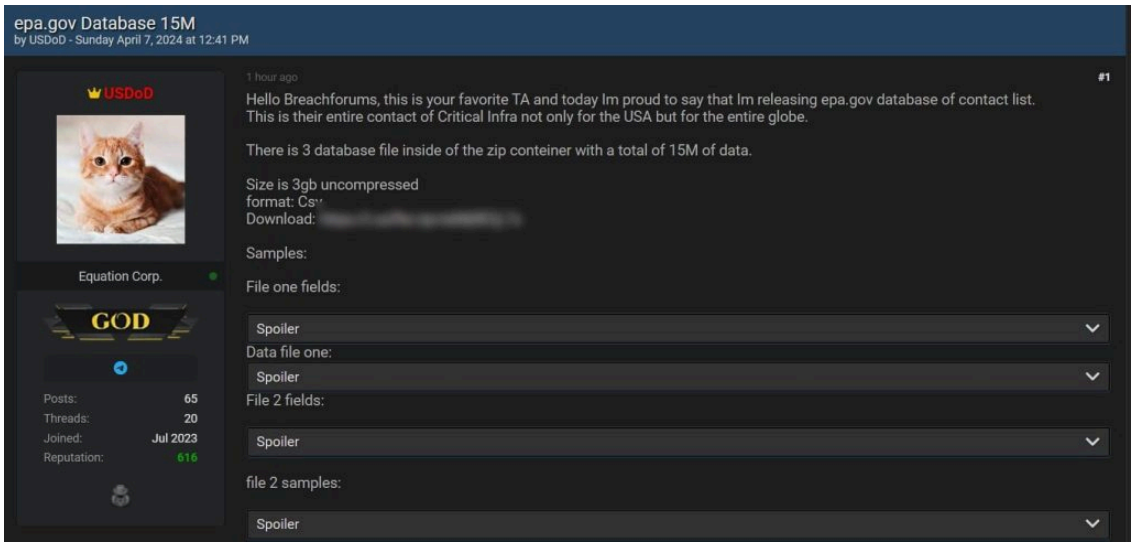
This article has been updated to include a statement from CISA and a response from the hacker.

The U.S. Environmental Protection Agency (EPA) is facing a data leak, carried out by a hacker operating under the alias USDoD. This data leak has exposed personal and sensitive information belonging to more than 8.5 million users, including customers and contractors.

The data breach was brought to light on the morning of Sunday, April 7, 2024. Notably, USDoD has a history of engaging in high-profile data breaches, with previous incidents including the exposure of data from **87,000 members of InfraGard**, a sensitive security program funded by the FBI and dedicated to safeguarding critical infrastructure in the United States.

> *"Hello Breachforums, this is your favorite TA and today Im proud to say that Im releasing epa.gov database of contact list. This is their entire contact of Critical Infra not only for the USA but for the entire globe."*
>
> *USDoD*

Regarding the data leak, the hacker told Hackread.com that the leak contains the entire contact database of the agency. Analysis conducted by Hackread.com indicates that the data provided by USDoD appears to be legitimate; however, conclusive verification can only be provided by the U.S. Environmental Protection Agency.



USDoD on Breach Forums (Screenshot credit: Hackread.com)

Meanwhile, a review of the leaked file reveals a 500MB Zip archive containing three CSV files labelled “Contact,” “Inter_Contact,” and “Staff.” An assessment of these files reveals the presence of the following information:

Contact File (3,726,130 Records)

- Zipcodes
- Full names
- Fax numbers
- Phone numbers
- Email addresses
- Mailing addresses
- Country, city, States

Inter_Contact File (9,952,374 Records)

- Zipcodes
- Full names
- Phone numbers
- Email addresses
- Email domains
- Country, City, State
- Company name and address

Staff File (3,325,973 Records)

- Zipcodes
- Fill names
- Job titles
- Company names
- Email addresses
- Business Addresses
- Phone numbers
- Related industries
- Country, city and States

Following the removal of duplicate records, the total number of accounts involved in the breach stands at nearly 8.5 million, specifically 8,460,182.

Screenshot from the leaked data (Credit: Hackread.com)

Hackread.com has notified the U.S. Environmental Protection Agency (EPA) and CISA regarding the data breach. Any response from either agency will lead to an update to this article.

UPDATE

UPDATE: 22:02 Monday, 8 April 2024 (GMT) – CISA has responded to Hackread.com confirming that the incident has been investigated by the FBI and the leaked data is already publicly available.

> *"FBI engaged EPA on Friday 4/5 where EPA determined the data reportedly taken as publicly available and the reported compromise to be a non-issue, per their internal hunting elements."*

> *CISA*

USDoD's Response

During a conversation with Hackread.com, the hacker stated that they never breached the EPA and that the data was indeed publicly available. They claimed to have extracted it from a Philadelphia-based third-party platform called DataRefuge.

The hacker also admitted that their post on Breach Forums should have clarified that there was no data breach of the EPA involved in the incident. However, they emphasized that the data is 100% authentic and of high importance, comparable to if an agency had been breached.

The Good and Bad news

The good news amidst this breach is the absence of passwords. However, the seriousness of the situation can be understood by the fact that the leaked data is now circulating within Russian hacker and cybercrime forums.

Devastating First Quarter of 2024 for US So Far

The first quarter of 2024 has proven to be quite challenging for the United States, a nation that holds influential global power and consequently becomes an attractive target for cybercriminals. Despite **ongoing efforts to strengthen its critical infrastructure**, the country has faced a surge in successful cyber attacks, resulting in widespread disruption and compromise.

In January, EquiLend, a prominent financial technology firm, fell victim to a large-scale ransomware attack. As a result, **it was confirmed that** the incident also led to a data breach, exposing sensitive employee information.

March witnessed the cyber attack from **IntelBroker hacker against Acuity Inc**., a federal contractor, resulting in the exposure of critical records belonging to U.S. Citizenship and Immigration Services (USCIS) and U.S. Immigration and Customs Enforcement (ICE). Although initially denied, Acuity Inc. eventually **acknowledged the hack**.

In February, the same hacker targeted the security of Los Angeles International Airport, compromising the personal data of 2.5 million private plane owners. Shortly thereafter, **in March**, American Express disclosed a significant data breach involving third-party contractors, impacting its cardholders.

The latest alleged data breach occurred **on April 4, 2024**, when the IntelBroker hacker leaked personal data belonging to over 22,000 Home Depot employees on BreachForums.

1. Data Sec: Congress Bans Staff Use of Microsoft's AI Copilot
2. US, China Exposed Most Databases Among 308,000 Found
3. Sony Data Breach via MOVEit Flaw Affects Thousands in US
4. Vietnamese DarkGate Malware Targets META Accounts in US
5. Adobe ColdFusion Flaw Used by Hackers to Access US Govt Servers

---

Source: https://www.hackread.com/us-environmental-protection-agency-hacked-data-leaked/