EYE OF LIBERTY · CONFIDENTIAL

DATA BREACH & OSINT AUDIT REPORT

Individual · OSINT Investigation

SUBJECT	Graham Cluley
PHONE	07510090891
EMAIL	graham@grahamcluley.com
REPORT ID	PVL-PHY-20260407
DATE	07.04.2026
SUBJECT TYPE	Individual

1. EXECUTIVE SUMMARY

During an automated OSINT investigation conducted by Eye of Liberty on 07.04.2026, data breach information for the subject was retrieved and verified. A total of **27 findings** were identified: **9 critical**, **10 high**, **2 medium**, **6 low**.

9	10	2	6
CRITICAL	HIGH	MEDIUM	LOW

2. SUBJECT INFORMATION

FULL NAME	Graham Cluley
PHONE	07510090891
EMAIL	graham@grahamcluley.com
SUBJECT TYPE	Individual
REPORT ID	PVL-PHY-20260407
DATE CHECKED	07.04.2026

3. INVESTIGATION FINDINGS

Findings are sorted by severity. All data was retrieved in real time on the report date.

F-001 **Database breach: 123RF** CRITICAL

SOURCE	QUERY	DATE CHECKED
LeakOSINT · 123RF	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «123RF». In March 2020, the 123RF stock photo site was leaked, which touched more than 8 million subscribers and was subsequently sold on the Internet. The leak included e -mail, IP, physical addresses, names, phones and passwords in the form of hashe MD5. Records found: 1.

COUNTRY	GB
COUNTRY	GB
EMAIL	graham@grahamcluley.com
NAME	Graham
IP ADDRESS	87.115.185.124
NAME	Cluley
PASSWORD	e3a1e7e036bec52f649c29ddde14a18d
REGDATE	2014-03-17

✓ **Recommendation:** Immediately change the password on the compromised service and on all accounts where the same or similar password was used. Enable two-factor authentication (preferably via an authenticator app, not SMS). Review login history and active sessions on affected accounts — terminate any unrecognized sessions immediately.

F-002 **Database breach: CafePress** CRITICAL

SOURCE	QUERY	DATE CHECKED
LeakOSINT · CafePress	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «CafePress». In February 2019, the retail seller of goods to order CafePress was led. 23 million posts were discovered. Some records contain names, physical addresses, phones and passwords in the form of hashe-1 hashes. Records found: 1.

COUNTRY	US
EMAIL	graham@grahamcluley.com
LASTACTIVE	May 13 2016 10
USERNAME	Stupid question
PASSWORD	7PBtTdN9TN0ziWXjZmatJ0lLttw=
REGDATE	May 13 2016 10

✓ **Recommendation:** Immediately change the password on the compromised service and on all accounts where the same or similar password was used. Enable two-factor authentication (preferably via an authenticator app, not SMS). Review login history and active sessions on affected accounts — terminate any unrecognized sessions immediately.

F-003 **Database breach: Cit0Day** CRITICAL

SOURCE	QUERY	DATE CHECKED
LeakOSINT · Cit0Day	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «Cit0Day». CIT0DAY is an now non -existent service for the search for e -mail among various leaks. After its closure in November 2020, a collection of more than 23,000 hacked sites fell into open access. The data was sorted into several dozen categories and contained more than 226 million posts and passwords to them. Some passwords were protected with the help of hashes. Records found: 13.

CATEGORY	Sports
EMAIL	graham@grahamcluley.com
LEAKSITE	hifkfans.com
PASSWORD	$2a$10$u7Y1/gi3VtOa3KlE3HonYOGYR3hANm7F75Ob1Nro9B3Zn2ZrCy25.
PASSWORD	PB22x52EBuYUdNsYf2rzbMuYF6DU5kj.
PASSWORD	61af9f53dfae54aac5c7c2d71db29d05
PASSWORD	ea0eccda4b02e26f67c5422013e6a34c
SALT	EqXkAI5PUrLTAtC6Qj6cBgdWptqnDbh1

✓ **Recommendation:** Immediately change the password on the compromised service and on all accounts where the same or similar password was used. Enable two-factor authentication (preferably via an authenticator app, not SMS). Review login history and active sessions on affected accounts — terminate any unrecognized sessions immediately.

F-004 Database breach: Cloudata

CRITICAL

SOURCE	QUERY	DATE CHECKED
LeakOSINT · Cloudata	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «Cloudata». Large collection of Email Pass data. The base was collected from many files on May 18, 2023. Initially, all bases weighed 338 GB (11 billion lines). After removing duplicates and data from the collections, about 2 billion remained. Records found: 1.

EMAIL	graham@grahamcluley.com
PASSWORD	2017-04-11

✓ **Recommendation:** Immediately change the password on the compromised service and on all accounts where the same or similar password was used. Enable two-factor authentication (preferably via an authenticator app, not SMS). Review login history and active sessions on affected accounts — terminate any unrecognized sessions immediately.

F-005 Database breach: Collection #1

CRITICAL

SOURCE	QUERY	DATE CHECKED
LeakOSINT · Collection #1	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «Collection #1». In January 2019, 5 collections appeared at the popular hacker forum, which are a combination of data from many other leaks. This is the first of the found collections. It contained 12.300 files with a total size of 87 GB. The collection has more than 2.5 billion lines with posts and passwords from them. There were only 1.25 billion unique lines. For many lines, a site was indicated on which a leak occurred. Records found: 2.

EMAIL	graham@grahamcluley.com
LEAKSITE	hifkfans.com (Sports)
PASSWORD	$2a$10$u7Y1/gi3VtOa3KlE3HonYOGYR3hANm7F75Ob1Nro9B3Zn2ZrCy25.

✓ **Recommendation:** Immediately change the password on the compromised service and on all accounts where the same or similar password was used. Enable two-factor authentication (preferably via an authenticator app, not SMS). Review login history and active sessions on affected accounts — terminate any unrecognized sessions immediately.

F-006 Database breach: Collection #2

CRITICAL

SOURCE	QUERY	DATE CHECKED
LeakOSINT · Collection #2	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «Collection #2». In January 2019, 5 collections appeared at the popular hacker forum, which are a combination of data from many other leaks. This is the second collection, it was the largest of all and contained 20 thousand files with a total size of 526 GB. These files had 15.8 billion lines with posts and passwords, but only 3.2 billion were unique pairs. Records found: 3.

EMAIL	graham@grahamcluley.com
PASSWORD	$2a$10$u7Y1/gi3VtOa3KlE3HonYOGYR3hANm7F75Ob1Nro9B3Zn2ZrCy25.
PASSWORD	b4be76a6f44e159f8e1159c49a1e425b
PASSWORD	wb9t7Jf9fE

✓ **Recommendation:** Immediately change the password on the compromised service and on all accounts where the same or similar password was used. Enable two-factor authentication (preferably via an authenticator app, not SMS). Review login history and active sessions on affected accounts — terminate any unrecognized sessions immediately.

F-007 Database breach: TeraBase64

CRITICAL

SOURCE	QUERY	DATE CHECKED
LeakOSINT · TeraBase64	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «TeraBase64». A huge collection of files, published in February 2020 by a man with a pseudonym @httsmvkcom. It contained 3.2 billion lines with mail and passwords in the form of a simple text, but there were only 1.28 billion unique lines. All these data were most likely obtained from many other leaks. Records found: 1.

EMAIL	graham@grahamcluley.com
PASSWORD	wb9t7Jf9fE

✓ **Recommendation:** Immediately change the password on the compromised service and on all accounts where the same or similar password was used. Enable two-factor authentication (preferably via an authenticator app, not SMS). Review login history and active sessions on affected accounts — terminate any unrecognized sessions immediately.

F-008 **Known vulnerabilities (NIST NVD): 52.14.244.175** CRITICAL

SOURCE	QUERY	DATE CHECKED
NIST NVD · 52.14.244.175	52.14.244.175	2026-04-07

For IP address «52.14.244.175», 18 vulnerabilities (CVEs) were found registered in the US National Vulnerability Database (NVD).

CVE-2023-40217	CVSS 5.3 (MEDIUM) — An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18, 3.10.x before 3.10.13, and 3.11.x before 3.11.5. It primarily affects servers (such as HTTP servers) that use TLS client authentication. If a TLS server-side socket is created, receives data into the socket buffer, and then is closed quickly, there is a brief window where the SSLSocket instance will detect the socket as "not connected" and won't initiate a handshake, but buffered data will still be readable from the socket buffer. This data will not be authenticated if the server-side TLS peer is expecting client certificate authentication, and is indistinguishable from valid TLS stream data. Data is limited in size to the amount that will fit in the buffer. (The TLS connection cannot directly be used for data exfiltration because the vulnerable code path requires that the connection be closed on initialization of the SSLSocket.)
CVE-2024-7592	CVSS 7.5 (HIGH) [CWE-400, CWE-1333] — There is a LOW severity vulnerability affecting CPython, specifically the 'http.cookies' standard library module. When parsing cookies that contained backslashes for quoted characters in the cookie value, the parser would use an algorithm with quadratic complexity, resulting in excess CPU resources being used while parsing the value.
CVE-2023-36632	CVSS 7.5 (HIGH) [CWE-674] — The legacy email.utils.parseaddr function in Python through 3.11.4 allows attackers to trigger "RecursionError: maximum recursion depth exceeded while calling a Python object" via a crafted argument. This argument is plausibly an untrusted value from an application's input data that was supposed to contain a name and an e-mail address. NOTE: email.utils.parseaddr is categorized as a Legacy API in the documentation of the Python email package. Applications should instead use the email.parser.BytesParser or email.parser.Parser class. NOTE: the vendor's perspective is that this is neither a vulnerability nor a bug. The email package is intended to have size limits and to throw an exception when limits are exceeded; they were exceeded by the example demonstration code.
CVE-2023-24329	CVSS 7.5 (HIGH) [CWE-20] — An issue in the urllib.parse component of Python before 3.11.4 allows attackers to bypass blocklisting methods by supplying a URL that starts with blank characters.
CVE-2009-3720	CVSS 5.0 () — The updatePosition function in lib/xmltok_impl.c in libexpat in Expat 2.0.1, as used in Python, PyXML, w3c-libwww, and other software, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with crafted UTF-8 sequences that trigger a buffer over-read, a different vulnerability than CVE-2009-2625.
CVE-2025-13836	CVSS 7.5 (HIGH) [CWE-400] — When reading an HTTP response from a server, if no read amount is specified, the default behavior will be to use Content-

	Length. This allows a malicious server to cause the client to read large amounts of data into memory, potentially causing OOM or other DoS.
CVE-2025-13837	CVSS 5.5 (MEDIUM) [CWE-400] — When loading a plist file, the plistlib module reads data in size specified by the file itself, meaning a malicious file can cause OOM and DoS issues
CVE-2024-9287	CVSS 7.8 (HIGH) [CWE-428, CWE-77] — A vulnerability has been found in the CPython `venv` module and CLI where path names provided when creating a virtual environment were not quoted properly, allowing the creator to inject commands into virtual environment "activation" scripts (ie "source venv/bin/activate"). This means that attacker-controlled virtual environments are able to run commands when the virtual environment is activated. Virtual environments which are not created by an attacker or which aren't activated before being used (ie "./venv/bin/python") are not affected.
CVE-2025-12084	CVSS 5.3 (MEDIUM) [CWE-407] — When building nested elements using xml.dom.minidom methods such as appendChild() that have a dependency on _clear_id_cache() the algorithm is quadratic. Availability can be impacted when building excessively nested documents.
CVE-2023-30861	CVSS 7.5 (HIGH) [CWE-539] — Flask is a lightweight WSGI web application framework. When all of the following conditions are met, a response containing data intended for one client may be cached and subsequently sent by the proxy to other clients. If the proxy also caches `Set-Cookie` headers, it may send one client's `session` cookie to other clients. The severity depends on the application's use of the session and the proxy's behavior regarding cookies. The risk depends on all these conditions being met. 1. The application must be hosted behind a caching proxy that does not strip cookies or ignore responses with cookies. 2. The application sets `session.permanent = True` 3. The application does not access or modify the session at any point during a request. 4. `SESSION_REFRESH_EACH_REQUEST` enabled (the default). 5. The application does not set a `Cache-Control` header to indicate that a page is private or should not be cached. This happens because vulnerable versions of Flask only set the `Vary: Cookie` header when the session is accessed or modified, not when it is refreshed (re-sent to update the expiration) without being accessed or modified. This issue has been fixed in versions 2.3.2 and 2.2.5.
CVE-2009-2940	CVSS 7.5 () — The pygresql module 3.8.1 and 4.0 for Python does not properly support the PQescapeStringConn function, which might allow remote attackers to leverage escaping issues involving multibyte character encodings.
CVE-2026-27205	CVSS 4.3 (MEDIUM) [CWE-524] — Flask is a web server gateway interface (WSGI) web application framework. In versions 3.1.2 and below, when the session object is accessed, Flask should set the Vary: Cookie header., resulting in a Use of Cache Containing Sensitive Information vulnerability. The logic instructs caches not to cache the response, as it may contain information specific to a logged in user. This is handled in most cases, but some forms of access such as the Python in operator were overlooked. The severity and risk depend on the application being hosted behind a caching proxy that doesn't ignore responses with cookies, not setting a Cache-Control header to mark pages as private or non-cacheable, and accessing the session in a way that only touches keys without reading values or mutating the session. The issue has been fixed in version 3.1.3.

CVE-2023-27043	CVSS 5.3 (MEDIUM) [CWE-20, CWE-1286] — The email module of Python through 3.11.3 incorrectly parses e-mail addresses that contain a special character. The wrong portion of an RFC2822 header is identified as the value of the addr-spec. In some applications, an attacker can bypass a protection mechanism in which application access is granted only after verifying receipt of e-mail to a specific domain (e.g., only @company.example.com addresses may be used for signup). This occurs in email/_parseaddr.py in recent versions of Python.
CVE-2025-12781	CVSS 5.3 (MEDIUM) [CWE-704] — When passing data to the b64decode(), standard_b64decode(), and urlsafe_b64decode() functions in the "base64" module the characters "+/" will always be accepted, regardless of the value of "altchars" parameter, typically used to establish an "alternative base64 alphabet" such as the URL safe alphabet. This behavior matches what is recommended in earlier base64 RFCs, but newer RFCs now recommend either dropping characters outside the specified base64 alphabet or raising an error. The old behavior has the possibility of causing data integrity issues. This behavior can only be insecure if your application uses an alternate base64 alphabet (without "+/"). If your application does not use the "altchars" parameter or the urlsafe_b64decode() function, then your application does not use an alternative base64 alphabet. The attached patches DOES NOT make the base64-decode behavior raise an error, as this would be a change in behavior and break existing programs. Instead, the patch deprecates the behavior which will be replaced with the newly recommended behavior in a future version of Python. Users are recommended to mitigate by verifying user-controlled inputs match the base64 alphabet they are expecting or verify that their application would not be affected if the b64decode() functions accepted "+" or "/" outside of altchars.
CVE-2021-32052	CVSS 6.1 (MEDIUM) [CWE-79] — In Django 2.2 before 2.2.22, 3.1 before 3.1.10, and 3.2 before 3.2.2 (with Python 3.9.5+), URLValidator does not prohibit newlines and tabs (unless the URLField form field is used). If an application uses values with newlines in an HTTP response, header injection can occur. Django itself is unaffected because HttpResponse prohibits newlines in HTTP headers.
CVE-2020-29396	CVSS 8.8 (HIGH) [CWE-267] — A sandboxing issue in Odoo Community 11.0 through 13.0 and Odoo Enterprise 11.0 through 13.0, when running with Python 3.6 or later, allows remote authenticated users to execute arbitrary code, leading to privilege escalation.
CVE-2024-6232	CVSS 7.5 (HIGH) [CWE-1333] — There is a MEDIUM severity vulnerability affecting CPython. Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives.
CVE-2007-4559	CVSS 9.8 (CRITICAL) [CWE-22] — Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.

✓ **Recommendation:** Update software on all affected services to the latest versions. Apply patches for critical CVEs immediately.

F-009 **Exploit probability (EPSS): 52.14.244.175** CRITICAL

SOURCE	QUERY	DATE CHECKED
FIRST EPSS · 52.14.244.175	52.14.244.175	2026-04-07

For IP address «52.14.244.175», EPSS (Exploit Prediction Scoring System) scores were obtained for 18 vulnerabilities. EPSS indicates the probability of a CVE being exploited in the next 30 days.

CVE-2007-4559	EPSS 90.58% (percentile 99.6%)
CVE-2024-6232	EPSS 4.02% (percentile 88.4%)
CVE-2021-32052	EPSS 2.57% (percentile 85.5%)
CVE-2020-29396	EPSS 1.81% (percentile 82.8%)
CVE-2023-24329	EPSS 1.59% (percentile 81.6%)
CVE-2009-3720	EPSS 1.54% (percentile 81.3%)
CVE-2024-7592	EPSS 1.02% (percentile 77.1%)
CVE-2023-40217	EPSS 0.60% (percentile 69.3%)
CVE-2009-2940	EPSS 0.58% (percentile 68.7%)
CVE-2025-13836	EPSS 0.20% (percentile 41.5%)
CVE-2023-30861	EPSS 0.19% (percentile 41.1%)
CVE-2023-27043	EPSS 0.18% (percentile 39.0%)
CVE-2023-36632	EPSS 0.08% (percentile 24.7%)
CVE-2024-9287	EPSS 0.06% (percentile 19.3%)
CVE-2025-12084	EPSS 0.06% (percentile 18.0%)
CVE-2025-13837	EPSS 0.04% (percentile 10.6%)
CVE-2025-12781	EPSS 0.02% (percentile 4.7%)
CVE-2026-27205	EPSS 0.01% (percentile 1.4%)

✓ **Recommendation:** Prioritize remediation of CVEs with high EPSS scores (>10%). These vulnerabilities are actively exploited or have a high probability of exploitation.

F-010 Database breach: Canva

HIGH

SOURCE	QUERY	DATE CHECKED
LeakOSINT · Canva	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «Canva». In May 2019, a data leak occurred on the web site of the CANVA graphic design tool. This leak affected 137 million subscribers. The disclosed data included mail, names, cities of residence and passwords in the form of Heshee Bcrypt. Records found: 1.

EMAIL	graham@grahamcluley.com
LANG	en
USERNAME	graham482
REGDATE	2015-09-08 21:39:25

✓ **Recommendation:** Leaked personal data (phone, address, full name) can be used for social engineering and account recovery attacks. Check whether this data is linked to password recovery on critical services (banking, email, government). Consider changing the phone number or email for your most important accounts.

F-011 Database breach: Epik.com Cleaned

HIGH

SOURCE	QUERY	DATE CHECKED
LeakOSINT · Epik.com Cleaned	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «Epik.com Cleaned». In September 2021, the registrar of domains and the EPIK web hosting leakage, presumably in revenge for placing alternative right websites. The leak revealed a huge amount of data, but they were poorly structured and very littered. Later, a cleaned version of this base appeared, which contains only mail and IP addresses, extracted from the original base using regular expressions. Records found: 1.

EMAIL	GRAHAM@GRAHAMCLULEY.COM

✓ **Recommendation:** Leaked personal data (phone, address, full name) can be used for social engineering and account recovery attacks. Check whether this data is linked to password recovery on critical services (banking, email, government). Consider changing the phone number or email for your most important accounts.

F-012 Database breach: Gravatar

HIGH

SOURCE	QUERY	DATE CHECKED
LeakOSINT · Gravatar	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «Gravatar». In October 2020, a methodology for extracting large volumes of data from Gravatar was published. This service provides common avatars for all sites. With the help of this method, 167 million names of users and hash MD5 their email addresses were collected. These hashes were used as a link to user avatars. Many hashs managed to decipher subsequently. Records found: 1.

AVATAR	https://secure.gravatar.com/avatar/aa9ea0686c5d1aa9086d4b12c3aa05f2
IP ADDRESS	Graham Cluley is a veteran of the anti-virus industry having worked for a number of security companies since the early 1990s when he wrote the first ever version of Dr Solomon's Anti-Virus Toolkit for Windows. Now an independent security analyst, he regularly makes media appearances and gives presentations on the topic of computer security and online privacy.
EMAIL	graham@grahamcluley.com
NAME	Graham
NAME	Cluley
LINK	http://gravatar.com/grahamcluley
USERNAME	Graham Cluley
USERNAME	grahamcluley
TITLE	Graham Cluley Security News

✓ **Recommendation:** Leaked personal data (phone, address, full name) can be used for social engineering and account recovery attacks. Check whether this data is linked to password recovery on critical services (banking, email, government). Consider changing the phone number or email for your most important accounts.

F-013 Database breach: Gravatar scrape 2023

HIGH

SOURCE	QUERY	DATE CHECKED
LeakOSINT · Gravatar scrape 2023	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «Gravatar scrape 2023». The Gravatar service allows users to use one avatar on many services. In January 2023, with the help of scraping, 61 million users were collected from it. They included mail, nicknames and avatars. Records found: 1.

AVATAR	https://secure.gravatar.com/avatar/aa9ea0686c5d1aa9086d4b12c3aa05f2
IP ADDRESS	Graham Cluley is a veteran of the anti-virus industry having worked for a number of security companies since the early 1990s when he wrote the first ever version of Dr Solomon's Anti-Virus Toolkit for Windows. Now an independent security analyst, he regularly makes media appearances and gives presentations on the topic of computer security and online privacy.
EMAIL	graham@grahamcluley.com
NAME	Graham
NAME	Cluley
USERNAME	grahamcluley
SITE	http://www.grahamcluley.com
TITLE	Graham Cluley Security News

✓ **Recommendation:** Leaked personal data (phone, address, full name) can be used for social engineering and account recovery attacks. Check whether this data is linked to password recovery on critical services (banking, email, government). Consider changing the phone number or email for your most important accounts.

F-014 Database breach: Onliner Spambot

HIGH

SOURCE	QUERY	DATE CHECKED
LeakOSINT · Onliner Spambot	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «Onliner Spambot». In August 2017, the Spam-Bot called "Onliner Spambot" was identified by the Benkow Mokueq security researcher. The malware contained a server component located on the IP address in the Netherlands, which revealed a large number of files with personal information. It was 711 million unique mail, many of which were also accompanied by passwords. Records found: 1.

EMAIL	graham@grahamcluley.com
FILE	old_Valid_Valid.txt

✓ **Recommendation:** Leaked personal data (phone, address, full name) can be used for social engineering and account recovery attacks. Check whether this data is linked to password recovery on critical services (banking, email, government). Consider changing the phone number or email for your most important accounts.

F-015 Database breach: RoyalServ.ru

HIGH

SOURCE	QUERY	DATE CHECKED
LeakOSINT · RoyalServ.ru	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «RoyalServ.ru». RoyalServ.ru-Russian online store of musical instruments. In 2023, a leak occurred on this site, which affected the data of 14 thousand users. The leak contained complete names, addresses of residence, mail, phone numbers, payment data, as well as IP addresses and other data. Records found: 1.

EMAIL	graham@grahamcluley.com

✓ **Recommendation:** Leaked personal data (phone, address, full name) can be used for social engineering and account recovery attacks. Check whether this data is linked to password recovery on critical services (banking, email, government). Consider changing the phone number or email for your most important accounts.

F-016 Database breach: Socradar Emails

HIGH

SOURCE	QUERY	DATE CHECKED
LeakOSINT · Socradar Emails	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «Socradar Emails». Socradar is a leak monitoring tool. In 2024, a list of 280 million emails allegedly received from this site appeared online. There is no other data except emails in the leak. Records found: 1.

EMAIL	graham@grahamcluley.com

✓ **Recommendation:** Leaked personal data (phone, address, full name) can be used for social engineering and account recovery attacks. Check whether this data is linked to password recovery on critical services (banking, email, government). Consider changing the phone number or email for your most important accounts.

F-017 Database breach: VerificationsIO

HIGH

SOURCE	QUERY	DATE CHECKED
LeakOSINT · VerificationsIO	graham@grahamcluley.com	2026-04-07

Identifier «graham@grahamcluley.com» (email) found in database «VerificationsIO». In February 2019, the Verifications.io post checks service suffered. Data in Mongodb were left in the public domain without a password, which opened 763 million unique mail, phones and IP. The data did not include passwords. Records found: 1.

EMAIL	graham@grahamcluley.com

✓ **Recommendation:** Leaked personal data (phone, address, full name) can be used for social engineering and account recovery attacks. Check whether this data is linked to password recovery on critical services (banking, email, government). Consider changing the phone number or email for your most important accounts.

F-018 Database breach: Luxottica

HIGH

SOURCE	QUERY	DATE CHECKED
LeakOSINT · Luxottica	07510090891	2026-04-07

Identifier «07510090891» (phone) found in database «Luxottica». Somewhere in November 2022, the Leader in the field of premium, luxurious and sports glasses with more than 7,400 stores in North America leaky data. This revealed the email addresses, phone numbers, date of birth, home addresses and complete names of buyers of the Luxottica brand. The leak occurred due to the fact that the third party revealed the data through a publicly available container for storage. Records found: 1.

EMAIL	GRAHAMCLULEY@BTINTERNET.COM
NAME	Graham
NAME	Cluley
PHONE	07510090891

✓ **Recommendation:** Leaked personal data (phone, address, full name) can be used for social engineering and account recovery attacks. Check whether this data is linked to password recovery on critical services (banking, email, government). Consider changing the phone number or email for your most important accounts.

F-019 **Home network indexed: 52.14.244.175** HIGH

SOURCE	QUERY	DATE CHECKED
Shodan Internet Scanner · 52.14.244.175	52.14.244.175	2026-04-07

IP address 52.14.244.175 (ISP: Amazon.com, Inc.) is indexed by Shodan with 1 open ports visible from the internet. Shodan recorded 18 known CVEs: CVE-2023-40217, CVE-2024-7592, CVE-2023-36632, CVE-2023-24329, CVE-2009-3720....

PORT 443	HTTPS
CVE / VULNERABILITIES	CVE-2023-40217, CVE-2024-7592, CVE-2023-36632, CVE-2023-24329, CVE-2009-3720, CVE-2025-13836, CVE-2025-13837, CVE-2024-9287, CVE-2025-12084, CVE-2023-30861, CVE-2009-2940, CVE-2026-27205, CVE-2023-27043, CVE-2025-12781, CVE-2021-32052, CVE-2020-29396, CVE-2024-6232, CVE-2007-4559
SHODAN TAGS	cloud
ISP	Amazon.com, Inc.
ORGANISATION	Amazon Technologies Inc.
GEOLOCATION	Columbus, United States
HOSTNAMES	ec2-52-14-244-175.us-east-2.compute.amazonaws.com, test.amalgam.me
LAST SCAN	2026-04-07T13:06:47.016235
CPE (DEVICE IDENTIFIERS)	cpe:/a:palletsprojects:flask:2.2.3, cpe:/a:python:python:3.10.9, cpe:2.3:a:palletsprojects:flask:2.2.3, cpe:2.3:a:python:python:3.10.9
HISTORY: PORT 443 / 2026-04-07	tcp

✓ **Recommendation:** Leaked personal data (phone, address, full name) can be used for social engineering and account recovery attacks. Check whether this data is linked to password recovery on critical services (banking, email, government). Consider changing the phone number or email for your most important accounts. Regularly check your home IP on shodan.io and keep router firmware updated.

F-020 Public Gravatar profile

MEDIUM

SOURCE	QUERY	DATE CHECKED
Gravatar · graham@grahamcluley.com	graham@grahamcluley.com	2026-04-07

Email «graham@grahamcluley.com» is linked to a public Gravatar profile. The profile contains personal information accessible to anyone who knows the email address.

DISPLAY NAME	Graham Cluley
PROFILE URL	https://gravatar.com/grahamcluley
ABOUT	Graham Cluley is an award-winning cybersecurity expert and keynote speaker. Since the early 1990s, he has worked in senior roles for major cybersecurity companies, regularly appeared in the media, and
LINKED ACCOUNTS	threads: https://threads.net/gcluley, twitter: https://x.com/gcluley, linkedin: https://www.linkedin.com/in/grahamcluley, tiktok: https://tiktok.com/@gcluley

✓ **Recommendation:** Review your Gravatar profile privacy settings at gravatar.com. Remove unnecessary personal information and unlink unused accounts.

F-021 Public Gravatar profile

MEDIUM

SOURCE	QUERY	DATE CHECKED
Gravatar · GRAHAM@GRAHAMCLULEY.COM	GRAHAM@GRAHAMCLULEY.COM	2026-04-07

Email «GRAHAM@GRAHAMCLULEY.COM» is linked to a public Gravatar profile. The profile contains personal information accessible to anyone who knows the email address.

DISPLAY NAME	Graham Cluley
PROFILE URL	https://gravatar.com/grahamcluley
ABOUT	Graham Cluley is an award-winning cybersecurity expert and keynote speaker. Since the early 1990s, he has worked in senior roles for major cybersecurity companies, regularly appeared in the media, and
LINKED ACCOUNTS	threads: https://threads.net/gcluley, twitter: https://x.com/gcluley, linkedin: https://www.linkedin.com/in/grahamcluley, tiktok: https://tiktok.com/@gcluley

✓ **Recommendation:** Review your Gravatar profile privacy settings at gravatar.com. Remove unnecessary personal information and unlink unused accounts.

F-022 IP reputation: AbuseIPDB

LOW

SOURCE	QUERY	DATE CHECKED
AbuseIPDB · 52.14.244.175	52.14.244.175	2026-04-07

IP address «52.14.244.175» checked against AbuseIPDB abuse reports database. Abuse confidence score: 0%.

ABUSE CONFIDENCE (ABUSEIPDB)	0%
USAGE TYPE (ABUSEIPDB)	Data Center/Web Hosting/Transit

✓ **Recommendation:** A high abuse score means malicious activity was reported from this IP. If this is your IP, scan all devices on the home network for malware and botnet agents, update router firmware, and change the Wi-Fi password. If the IP is dynamic, it may have been compromised by a previous user.

F-023 IP antivirus analysis: VirusTotal

LOW

SOURCE	QUERY	DATE CHECKED
VirusTotal · 52.14.244.175	52.14.244.175	2026-04-07

IP address «52.14.244.175» checked via VirusTotal antivirus aggregator. 0 engines flagged the address as malicious.

DETECTIONS (VIRUSTOTAL)	0 malicious, 0 suspicious / 94 engines

✓ **Recommendation:** VirusTotal antivirus engines flagged this IP as suspicious. Scan all devices on your network, update router firmware, and ensure the router admin password is not set to default. If malicious detections are present, consider requesting a new IP from your ISP.

F-024 Geolocation and network: ipinfo.io

LOW

SOURCE	QUERY	DATE CHECKED
ipinfo.io · 52.14.244.175	52.14.244.175	2026-04-07

Network information for IP address «52.14.244.175» retrieved from ipinfo.io.

ASN (IPINFO)	AS16509
AS NAME (IPINFO)	Amazon.com, Inc.
COUNTRY (IPINFO)	United States

✓ **Recommendation:** Verify that the geolocation and ISP match your actual location. A mismatch may indicate third-party use of your IP or spoofed data in the breach. If you are not using a VPN and the country/city don't match, this warrants further investigation.

F-025 Network scan (Nmap): 52.14.244.175

LOW

SOURCE	QUERY	DATE CHECKED
Nmap · 52.14.244.175	52.14.244.175	2026-04-07

Active scan of IP address «52.14.244.175» found 1 open ports. No vulnerabilities detected.

PORT 443/TCP	http (Werkzeug httpd 2.2.3)

✓ **Recommendation:** Close all unused ports. Update services with detected vulnerabilities. Restrict access to administrative ports via firewall.

F-026 **Web server technologies: 52.14.244.175** LOW

SOURCE	QUERY	DATE CHECKED
WhatWeb · 52.14.244.175	52.14.244.175	2026-04-07

Web server «52.14.244.175» runs 6 detected technologies/components.

COOKIES	session
HTTPSERVER	Werkzeug/2.2.3 Python/3.10.9
HTTPONLY	session
PYTHON	3.10.9
UNCOMMONHEADERS	access-control-allow-origin
WERKZEUG	2.2.3

✓ **Recommendation:** Hide server version headers (Server, X-Powered-By). Update all detected components to current versions.

F-027 **TLS/SSL analysis: 52.14.244.175** LOW

SOURCE	QUERY	DATE CHECKED
testssl.sh · 52.14.244.175	52.14.244.175	2026-04-07

TLS/SSL configuration analysis on «52.14.244.175:443» found 31 issues.

ENGINE_PROBLEM	[WARN] No engine or GOST support via engine with your /usr/bin/openssl
TLS1	[LOW] offered (deprecated)
TLS1_1	[LOW] offered (deprecated)
CIPHERLIST_OBSOLETED	[LOW] offered
CIPHER-TLS1_XC013	[LOW] TLSv1 xc013 ECDHE-RSA-AES128-SHA ECDH 256 AES 128 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
CIPHER-TLS1_XC014	[LOW] TLSv1 xc014 ECDHE-RSA-AES256-SHA ECDH 256 AES 256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
CIPHER-TLS1_X2F	[LOW] TLSv1 x2f AES128-SHA RSA AES 128 TLS_RSA_WITH_AES_128_CBC_SHA
CIPHER-TLS1_X35	[LOW] TLSv1 x35 AES256-SHA RSA AES 256 TLS_RSA_WITH_AES_256_CBC_SHA
CIPHER-TLS1_1_XC013	[LOW] TLSv1.1 xc013 ECDHE-RSA-AES128-SHA ECDH 256 AES 128 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
CIPHER-TLS1_1_XC014	[LOW] TLSv1.1 xc014 ECDHE-RSA-AES256-SHA ECDH 256 AES 256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
CIPHER-TLS1_1_X2F	[LOW] TLSv1.1 x2f AES128-SHA RSA AES 128 TLS_RSA_WITH_AES_128_CBC_SHA
CIPHER-TLS1_1_X35	[LOW] TLSv1.1 x35 AES256-SHA RSA AES 256 TLS_RSA_WITH_AES_256_CBC_SHA
CIPHER-TLS1_2_XC027	[LOW] TLSv1.2 xc027 ECDHE-RSA-AES128-SHA256 ECDH 256 AES 128 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
CIPHER-TLS1_2_XC013	[LOW] TLSv1.2 xc013 ECDHE-RSA-AES128-SHA ECDH 256 AES 128 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
CIPHER-TLS1_2_XC028	[LOW] TLSv1.2 xc028 ECDHE-RSA-AES256-SHA384 ECDH 256 AES 256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

✓ **Recommendation:** Update TLS configuration: disable legacy protocols (TLS 1.0/1.1), weak ciphers, and renew certificates.

4. GENERAL RECOMMENDATIONS

Password Management	Never reuse the same password across different services. This protects you from credential stuffing attacks where adversaries use passwords from one breach to access other accounts. Use a trusted password manager (e.g. Bitwarden, KeePassXC, 1Password) to generate and securely store unique passwords for every service.
Account Protection	Immediately change all passwords flagged in this report, and any accounts where the same or similar password was used. Enable two-factor authentication (2FA) everywhere possible — prefer an authenticator app (Google Authenticator, Authy) over SMS, as SMS codes can be intercepted via SIM-swap attacks.
Digital Hygiene	Use separate email addresses and virtual/disposable phone numbers for low-trust services (delivery, marketplaces, loyalty programmes). Keep your primary phone number and email limited to critical accounts only. Review the privacy settings on your social media profiles and limit public visibility of personal information.
Fraud Awareness	Be aware that leaked data (your name, phone number, address, order history) can be used for social engineering. Treat any unsolicited calls claiming to be from a bank, law enforcement, or government authority with extreme caution — the fact that a caller knows your personal details does not make them legitimate.
Ongoing Monitoring	Periodically review active sessions in Telegram, WhatsApp, and other messaging apps — terminate any unrecognised sessions immediately. Subscribe to breach alerts via services such as Have I Been Pwned (haveibeenpwned.com). Consider ordering a follow-up audit from Eye of Liberty in 3–6 months to verify your improved security posture.

5. LEGAL DISCLAIMER

This report is provided for informational purposes only. All data has been obtained from publicly available sources in accordance with applicable law. Eye of Liberty accepts no liability for the use of the information contained in this document by third parties. This report is intended solely for the data subject or their authorised representative. Unauthorised copying, distribution or publication of this document is strictly prohibited. Privacy Policy: eyeofliberty.com/privacy