BACS 4499 Attack Observation Template

|  |  |  |
| --- | --- | --- |
| Time and Date of Activity | January 23, 2025, 1:03 - 2:16 | |
|  | | |
| Relevant Logs, File or Email   * Provide an Executive Summary of the Activity   + IP involved, account information (if exists)   + Gear this toward an audience of basic technical skills * Whenever available, provide a summary of the Relevant Activity using the Sensor log   + Include correlated Activity over Time   + TTY logs (if available) can be listed & explained in this section.   + Table, Graphs or Pictures to illustrate the AO.   + Traffic flow   + Malware Analysis   + Use DShield data to compare activity. * If you created a custom script for parsing the logs, you can explain it function here. | | |
| Executive Summary:  Between 1:03 PM - 2:16 PM UTC of January 23, 2025 a host (84.247.172.212) connected to my Dshield honeypot host 1,750,074 times attempting to brute force download 6894 files using an HTTP GET method. This information was enumerated from the Dshield Web Honey Pot Log (“webhoneypot-2025-01-23.json”). This attack is assumed to be automated with the use of a word list of common valuable files. | | |
| Which vulnerability does the attack attempt to exploit?   * Exploit * CVE * Mitre ATT&CK | | |
| This attempts to exploit a common misconfiguration of web servers that hosts more information than intended from the host operating systems directory structure.  Relevant / Related Mitre ATT&CK Techniques:  [**Active Scanning: Wordlist Scanning: T1595.003**](https://attack.mitre.org/techniques/T1595/003/)  [**Exploit Public-Facing Application: T1190**](https://attack.mitre.org/techniques/T1190/) | | |
| What is the goal of the attack? | | |
| The goal of the attack is to download as much information as possible from a misconfigured web server. This could be used as a method of reconnaissance for continued attack. This attack attempted to download the contents of 6,894 separate files that, if available, would help an attacker create additional attack vectors.  Most common files attempted to be exfiltrated:   |  |  | | --- | --- | | **URL** | **Connection attempts** | | /debug/default/view | 4489 | | /phpinfo | 1044 | | /library/.env | 982 | | /index.php | 804 | | /test.php | 782 | | /phpinfo.php | 782 | | /info.php | 744 | | /config.js | 737 | | /\_profiler/phpinfo | 697 | | /env.json | 687 | | /environment.ts | 681 | | / | 677 | | /settings.py | 674 | | /test1.php | 661 | | /test2.php | 660 | | | |
| If the system is vulnerable, do you think the attack will be successful? | | |
| Absolutely. | | |
| How can a system be protected from this attack? | | |
| Ensuring the web server is only hosting the content it should be. Disabling web indexing and ensuring path traversal is not possible. Additional recommend all publicly facing web servers be hardened in accordance with the appropriate hardening guidance for the environment it’s being hosted within. (CIS Benchmarks \ DISA STIG \ DISA SRG \ Application specific hardening guides) | | |
| What do you know about the attacker?   * References * ThreatIntel * Whois Information * [Shodan](https://www.shodan.io) * [CyberGordon](https://cybergordon.com) * [AlienVault](https://otx.alienvault.com) * [ISC](https://isc.sans.edu/ipinfo.html) | | |
| **Whois Information:**  Sorry, but RIPE blocks our requests. Please check directly at whois.ripe.net  NetRange: 84.0.0.0 - 84.255.255.255  CIDR: 84.0.0.0/8  NetName: 84-RIPE  NetHandle: NET-84-0-0-0-1  Parent: ()  NetType: Allocated to RIPE NCC  OriginAS:  Organization: RIPE Network Coordination Centre (RIPE)  RegDate: 2003-11-17  Updated: 2004-03-16  Comment: These addresses have been further assigned to users in  Comment: the RIPE NCC region. Contact information can be found in  Comment: the RIPE database at http://www.ripe.net/whois  Ref: https://rdap.arin.net/registry/ip/84.0.0.0  ResourceLink: https://apps.db.ripe.net/search/query.html  ResourceLink: whois.ripe.net  OrgName: RIPE Network Coordination Centre  OrgId: RIPE  Address: P.O. Box 10096  City: Amsterdam  StateProv:  PostalCode: 1001EB  Country: NL  RegDate:  Updated: 2013-07-29  Ref: https://rdap.arin.net/registry/entity/RIPE  ReferralServer: whois://whois.ripe.net  ResourceLink: https://apps.db.ripe.net/search/query.html  OrgAbuseHandle: ABUSE3850-ARIN  OrgAbuseName: Abuse Contact  OrgAbusePhone: +31205354444  OrgAbuseEmail: abuse@ripe.net  OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE3850-ARIN  OrgTechHandle: RNO29-ARIN  OrgTechName: RIPE NCC Operations  OrgTechPhone: +31 20 535 4444  OrgTechEmail: hostmaster@ripe.net  OrgTechRef: https://rdap.arin.net/registry/entity/RNO29-ARIN    **Shodan:** <https://www.shodan.io/host/84.247.172.212>  **General information:**   |  |  |  | | --- | --- | --- | | * Hostnames |  | vmi2395298.**contaboserver.net** | | * Domains |  | [contaboserver.net](https://www.shodan.io/domain/contaboserver.net) | | * Country |  | [**Germany**](https://www.shodan.io/search?query=country%3A%22DE%22) | | * City |  | [**Düsseldorf**](https://www.shodan.io/search?query=city%3A%22D%C3%BCsseldorf%22) | | * Organization |  | [**Contabo GmbH**](https://www.shodan.io/search?query=org%3A%22Contabo+GmbH%22) | | * ISP |  | [**Contabo GmbH**](https://www.shodan.io/search?query=isp%3A%22Contabo+GmbH%22) | | * ASN |  | [**AS51167**](https://www.shodan.io/search?query=asn%3A%22AS51167%22) |   **OpenPorts:**  **21, 22, 25, 53, 110, 993, 995, 8443, 8080**  **CyberGordon:** <https://cybergordon.com/r/11e35f54-d4f6-4d6f-9902-e9f3790fa143>  **ISC:** [**https://isc.sans.edu/ipinfo/84.247.172.212**](https://isc.sans.edu/ipinfo/84.247.172.212)  **General Information**   |  |  | | --- | --- | | Submitter Diversity: | Low | | Risk (0-10)[details](https://isc.sans.edu/ipinfo/risk.html): | 1 | | IP Address (click for more detail): | [84.247.172.212](https://isc.sans.edu/ipdetails.html?ip=84.247.172.212) | | Hostname: | vmi2395298.contaboserver.net | | Country: | DE | | AS: | [51167](https://isc.sans.edu/asreport.html?as=51167) | | AS Name: | CONTABO, DE | | Network: | 84.247.160.0/19 (84.247.160.0-84.247.191.255) 84.247.192.0 | | Reports: | [1636](https://isc.sans.edu/ipdetails.html?ip=84.247.172.212&1636) | | Targets: | 1 | | First Reported: | [2025-01-12](https://isc.sans.edu/date.html?date=2025-01-12) | | Most Recent Report: | [2025-01-28](https://isc.sans.edu/date.html?date=2025-01-28) | | Comment: | - none - | | Abuse POC Email: | abuse@contabo.de | | | |
| Indicators   * IP List * Hashes * Domain * URL * Yara | | |
| Source IP: 84.247.172.212 | | |
| External References   * [reference number] URL\resource | | |
| **References:**  Relevant / Related Mitre ATT&CK Techniques:  [**Active Scanning: Wordlist Scanning: T1595.003**](https://attack.mitre.org/techniques/T1595/003/)  [**Exploit Public-Facing Application: T1190**](https://attack.mitre.org/techniques/T1190/) | | |
|  | | |
| Analyst Name: Woodrow Moore | | Date of Analysis: 01/29/2025 |