Oct 15 2023

NETMANAGEIT

Intelligence Report

Critical Vulnerabilities: WS_FTP Exploitation

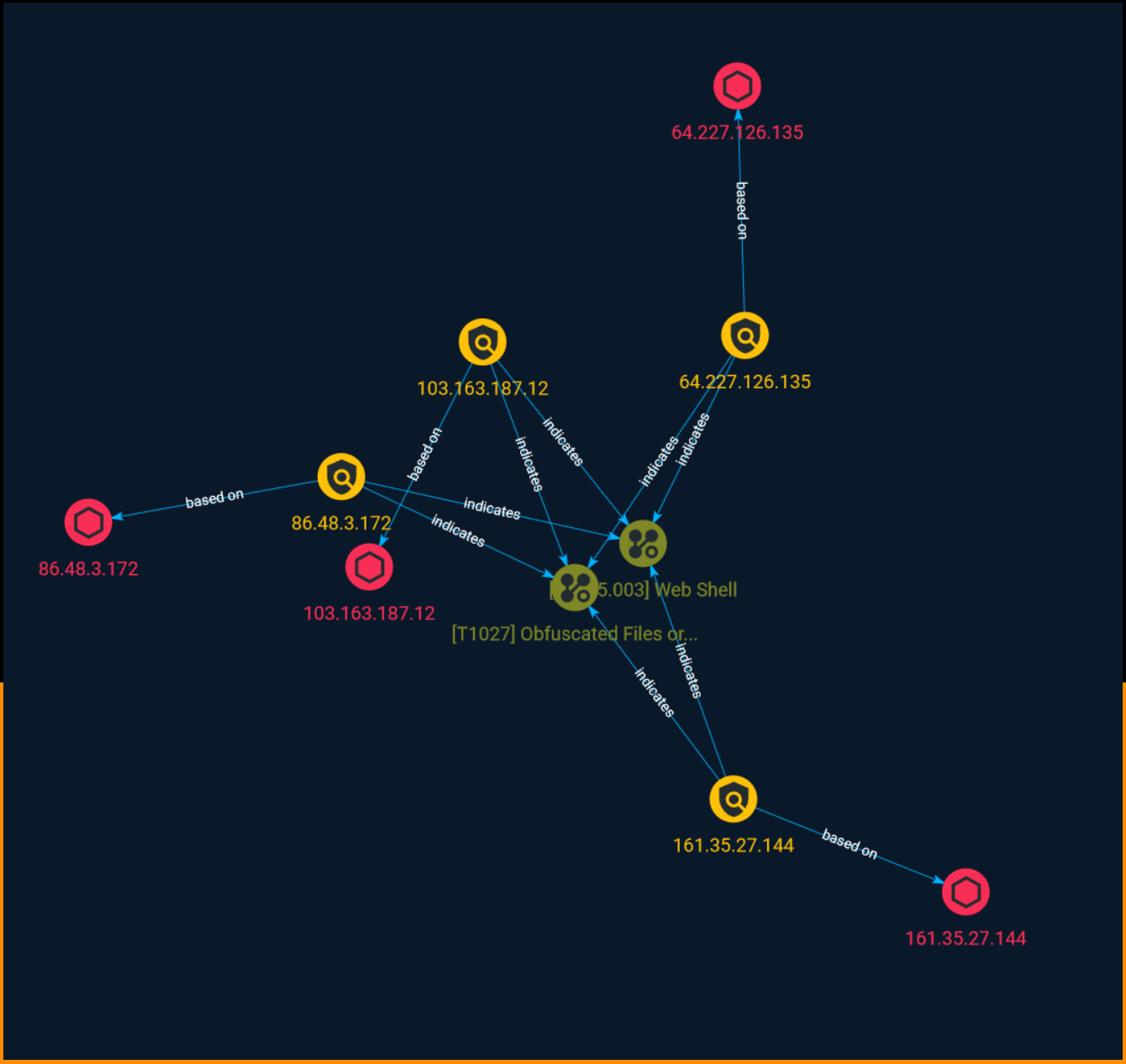

Table of contents

Overview

Entities

Observables

External References

Overview

Description

As disclosed by Progress, CVE-2023-40044 is the critical (CVSS: 10) remote code execution vulnerability that does not require authentication.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
Web Shell
ID
T1505.003
Description
Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server.(Citation: volexity_0day_sophos_FW) In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (e.g. [China Chopper](https://attack.mitre.org/software/S0020) Web shell client). (Citation: Lee 2013)
Name
Obfuscated Files or Information
ID
T1027
Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Indicator

Name

103.163.187.12

Description

ISP: SpeedyPage Ltd **OS:** Ubuntu ---------- Hostnames: - 12.187.163.103.speedyvps.uk ---------- Domains: - speedyvps.uk ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCmsh00Ma4dLEmPBwV8OynGvIAzXvcJPHxaZaXyesaiFxu+ bxQM1ycZrByIiUUG1AjGvxi11Y5jN8wQnenDnyLLllou882i1CZkDUg0W6xBk4FUSSwVklt0E4GEeIf9/yZyKF+z9tsHwnVqNWU/CpXgspEc9mkG4EGkBZIfM8cVP8JP/a6nNK9+JLWg1tlvc6kZ5bcNF2QAcVtXjRri7NtOZjWA/XN8X75YxBCnjJYqNBIWNSA8+qAv7SvaT6jW69++M6cUii+3gCq5zKBwKDphgt4Bj7SCAy8eKCpwCsTvruY87Fk0Fbed9Rvj0u+TeSQDgfx4EUwELOxujALOh0bz Fingerprint: 31:a0:f0:89:64:0b:54:57:e7:84:22:a0:92:96:2e:db Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Wed, 13 Sep 2023 21:53:19 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 13 Connection: keep-alive Cache-Control: no-cache, no-store, must-revalidate Expires: 0 Pragma: no-cache Vary: Accept-Encoding ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Wed, 06 Sep 2023 11:56:53 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 13 Connection: keep-alive Cache-Control: no-

cache, no-store, must-revalidate Expires: 0 Pragma: no-cache Vary: Accept-Encoding ``` HEARTBLEED: 2023/09/06 11:57:04 103.163.187.12:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.163.187.12']

Name

161.35.27.144

Description

Agressive IP known malicious on AbuseIPDB - countryCode: DE - abuseConfidenceScore: 100 - lastReportedAt: 2023-10-06T15:04:24+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '161.35.27.144']

Name

86.48.3.172

Description

ISP: Contabo GmbH **OS:** Debian ---------- Hostnames: - vmi1147584.contaboserver.net ---------- Domains: - contaboserver.net

---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAACAQC1/ZGiyQN13ulAPAeinB64MKXyPcus4EMVWZuwyIe0VAKV RXodqwdlhr5oWmH2X3pOl9bqJk3UCuOHzExybSJemMTU3VDOhc0s7YHlCSehnx1haPfdbXzjGYWp PpyUXOLBD3ftKNA5Hlhkl3pDVcq3tdiLDyOyYZiPX4wQQzc+ApzeXJJoOC78xQtqIbs6o9T5TWdw PhjhAGn8iZuHGclNCONwPOSPEuiqZYQsykIOizBgolhnrchJddmHaVZYhEoMpWw44h+krm5W8oDo Kftu2sXIbTpuhgWAOZpgfZpD5VAELcKj58SOVI8/kXLfzqiQ6xIYqfwrKfhPSlvOhahSfRoDtqYCs/eL6eOHoHXMFvsa9227e5ct5Mb9YZNQHV6AFsNKkzoV1sGbd2j74dSIFAYnMMLGVh3myNvuM1k2fy0dr9q6dpLtnOJeMAuc+JsMhq1Cj5Q6IQ77nAJsWpWdhvqlREL9JJbOrA32vM/J/V0fgiSs3VroaZ1UBxjdYw3+G7Y8KzwStynTyHGQj4vLyb5Tdxn30zaCnVuZi536dF4L+mQasTMFrUC0mgXVMcnM3yrpOB8MtZw/vYchrafTwyZFqnWlTM10PcUluqNsyuZIZQNni5fx1mCcUfjdKqWVb9anntX9EF9/j6py4aus0rZX7nbvoC4Kh3dKHFTKgQ== Fingerprint: 35:1b:e5:c6:58:f3:51:5c:d6:72:cd:38:1a:e0:bc:0d Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Tue, 12 Sep 2023 22:30:07 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Thu, 06 Apr 2023 19:19:14 GMT ETag: "2aa6-5f8afc8b914c2" Accept-Ranges: bytes Content-Length: 10918 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **631:** ``` HTTP/1.1 403 Forbidden Connection: close Content-Language: en Content-Length: 370 Content-Type: text/html; charset=utf-8 Date: Thu, 14 Sep 2023 04:02:42 GMT Accept-Encoding: gzip, deflate, identity Server: CUPS/2.4 IPP/2.1 X-Frame-Options: DENY Content-Security-Policy: frame-ancestors 'none' ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '86.48.3.172']

Name

64.227.126.135

Description

Agressive IP known malicious on AbuseIPDB - countryCode: DE - abuseConfidenceScore: 100 - lastReportedAt: 2023-10-07T15:03:49+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.227.126.135']

IPv4-Addr

Value
103.163.187.12
64.227.126.135
161.35.27.144
86.48.3.172

External References

- https://otx.alienvault.com/pulse/652855a131fde4769f70f324
- https://www.huntress.com/blog/critical-vulnerabilities-ws_ftp-exploitation