Oct 04 2023

NETMANAGEIT

Intelligence Report

They've begun: Attacks exploiting vulnerability with maximum 10 severity rating (CVE-2023-40044)

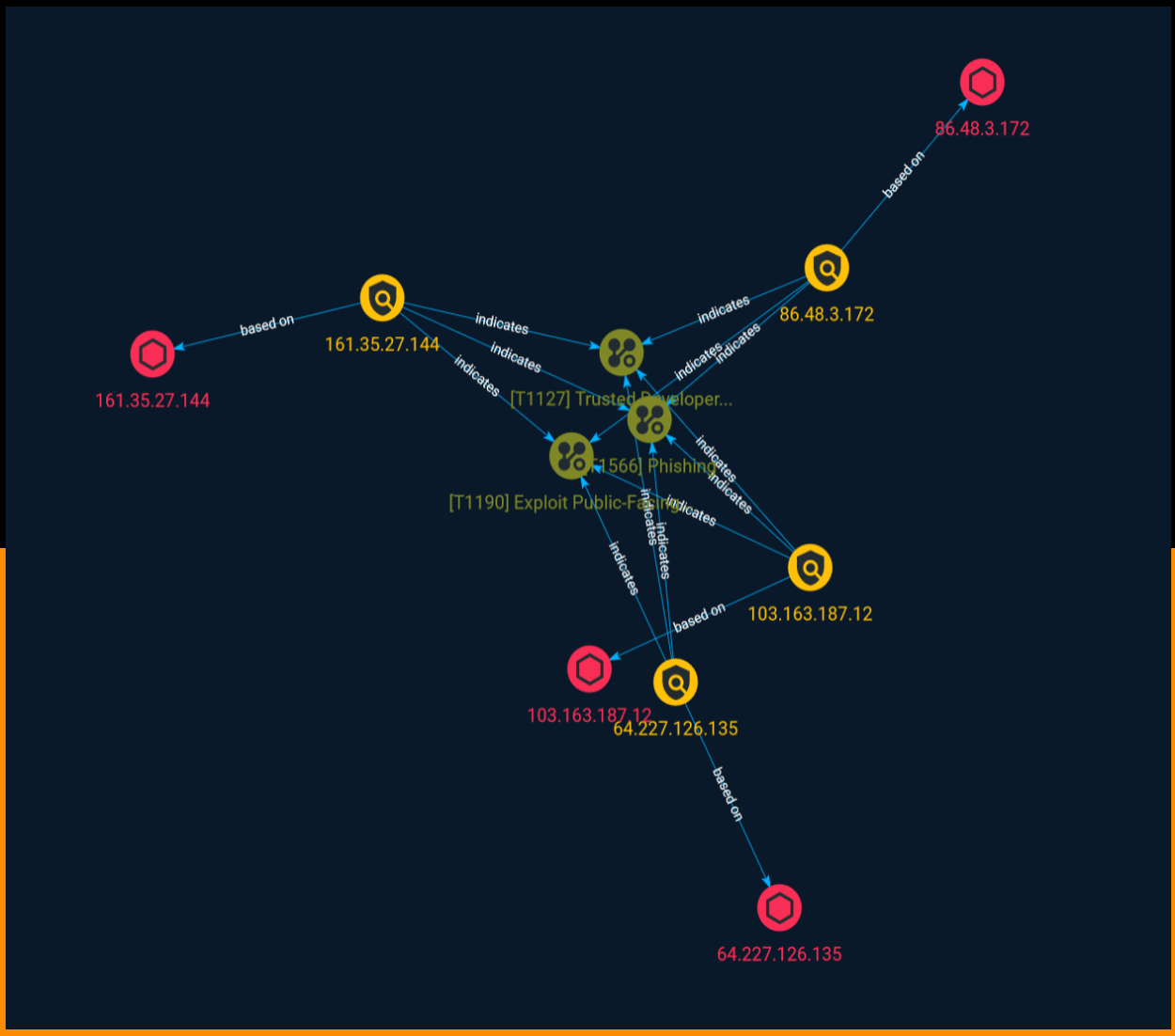

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Security researchers have warned that hackers are exploiting two critical vulnerabilities in file-transfer software, known as WS_FTP, that have led to the compromise of more than 3.4 million people.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Exploit Public-Facing Application

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Name

Trusted Developer Utilities Proxy Execution

ID

T1127

Description

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.(Citation: engima0x3 DNX Bypass)(Citation: engima0x3 RCSI Bypass)(Citation: Exploit Monday WinDbg)(Citation: LOLBAS Tracker) These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

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: 2023-09-27T15:03:39+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/ eL6eOHoHXMFvsa9227e5ct5Mb9YZNQHV6AFsNKkzoV1sGbd2j74dSIFAYnMMLGVh3myNvuM1k2 fy0dr9q6dpLtnOJeMAuc+JsMhq1Cj5Q6IQ77nAJsWpWdhvqlREL9JJbOrA32vM/J/V0fgiSs3Vro aZ1UBxjdYw3+G7Y8KzwStynTyHGQj4vLyb5Tdxn30zaCnVuZi536dF4L+mQasTMFrUC0mgXVMcnM 3yrpOB8MtZw/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: 2023-09-20T14:00:30+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/651d869e90bcd443460050ee
- https://arstechnica.com/security/2023/10/active-attacks-exploiting-ws_ftp-pose-a-grave-threat-to-the-internet/