May 10 2024

NETMANAGEIT

Intelligence Report

Protecting Networks from Opportunistic Ivanti Pulse Secure Vulnerability Exploitation

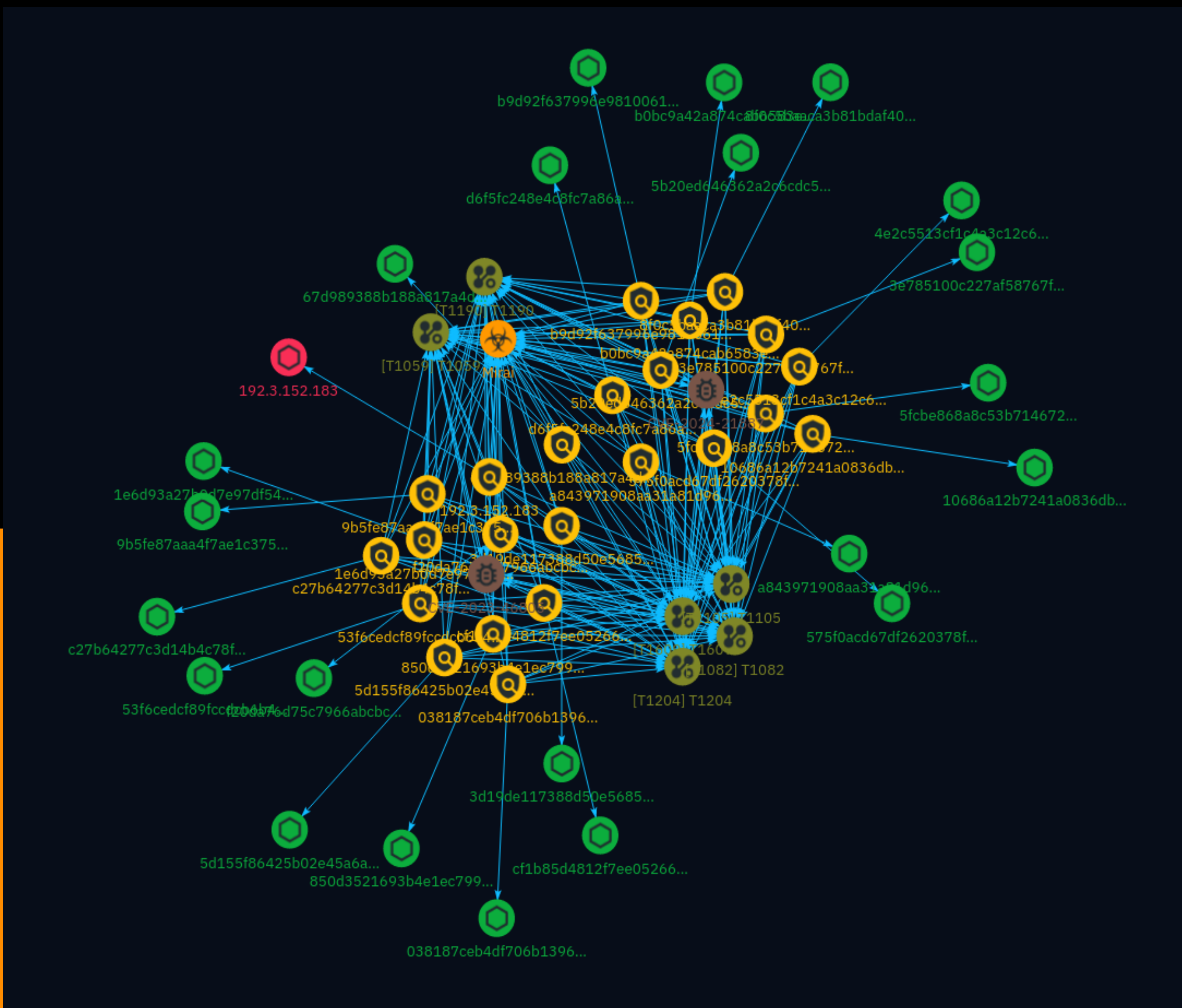

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Juniper Threat Labs has observed attempts to exploit Ivanti Pulse Secure authentication bypass and remote code execution vulnerabilities (CVE-2023-46805 and CVE-2024-21887), leading to the delivery of Mirai botnet payloads. This analysis explores the vulnerabilities, exploitation methods, observed payloads, and Juniper's response, highlighting the importance of understanding and mitigating these threats to protect network security.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
f20da76d75c7966abcbc050dde259a2c85b331c80cce0d113bc976734b78d61d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f20da76d75c7966abcbc050dde259a2c85b331c80cce0d113bc976734b78d61d']
Name
d6f5fc248e4c8fc7a86a8193eb970fe9503f2766951a3e4b8c084684e423e917
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd6f5fc248e4c8fc7a86a8193eb970fe9503f2766951a3e4b8c084684e423e917']
Name

b9d92f637996e981006173eb207734301ff69ded8f9c2a7f0c9b6d5fcc9063a2
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b9d92f637996e981006173eb207734301ff69ded8f9c2a7f0c9b6d5fcc9063a2']
Name
cf1b85d4812f7ee052666276a184b481368f0c0c7a43e6d5df903535f466c5fd
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'cf1b85d4812f7ee052666276a184b481368f0c0c7a43e6d5df903535f466c5fd']
Name
b0bc9a42a874cab6583e4993de7cc11a2b8343a4453bda97b83b0c2975e7181d
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'b0bc9a42a874cab6583e4993de7cc11a2b8343a4453bda97b83b0c2975e7181d']
Name
a843971908aa31a81d96cc8383dcde7f386050c6e3437ad6a470f43dc2bf894b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a843971908aa31a81d96cc8383dcde7f386050c6e3437ad6a470f43dc2bf894b']
Name
9b5fe87aaa4f7ae1c375276bfe36bc862a150478db37450858bbfb3fb81123c2
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '9b5fe87aaa4f7ae1c375276bfe36bc862a150478db37450858bbfb3fb81123c2']
Name
8f0c5baaca3b81bdaf404de8e7dcca1e60b01505297d14d85fea36067c2a0f14
Pattern Type

stix
Pattern
[file:hashes.'SHA-256' = '8f0c5baaca3b81bdaf404de8e7dcca1e60b01505297d14d85fea36067c2a0f14']
Name
850d3521693b4e1ec79981b3232e87b0bc22af327300dfdc7ea1b7a7e97619cd
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '850d3521693b4e1ec79981b3232e87b0bc22af327300dfdc7ea1b7a7e97619cd']
Name
67d989388b188a817a4d006503e5350a1a2af7eb64006ec6ad6acc51e29fdcd5
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '67d989388b188a817a4d006503e5350a1a2af7eb64006ec6ad6acc51e29fdcd5']
Name

5fcbe868a8c53b7146724d579ff82252f00d62049a75a04baa4476e300b42d15
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '5fcbe868a8c53b7146724d579ff82252f00d62049a75a04baa4476e300b42d15']
Name
5d155f86425b02e45a6a5d62eb8ce7827c9c43f3025bffd6d996aabd039d27f9
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '5d155f86425b02e45a6a5d62eb8ce7827c9c43f3025bffd6d996aabd039d27f9']
Name
5b20ed646362a2c6cdc5ca0a79850c7d816248c7fd5f5203ce598a4acd509f6b
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '5b20ed646362a2c6cdc5ca0a79850c7d816248c7fd5f5203ce598a4acd509f6b']

Name
575f0acd67df2620378fb5bd8379fd2f2ba0539b614986d60e85822ba0e9aa08
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '575f0acd67df2620378fb5bd8379fd2f2ba0539b614986d60e85822ba0e9aa08']

Name
53f6cedcf89fccdcb6b4b9c7c756f73be3e027645548ee7370fd3486840099c4
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '53f6cedcf89fccdcb6b4b9c7c756f73be3e027645548ee7370fd3486840099c4']

Name
3e785100c227af58767f253e4dfe937b2aa755c363a1497099b63e3079209800
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3e785100c227af58767f253e4dfe937b2aa755c363a1497099b63e3079209800']

Name

3d19de117388d50e5685d203683c2045881a92646c69ee6d4b99a71bf65dafa7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3d19de117388d50e5685d203683c2045881a92646c69ee6d4b99a71bf65dafa7']

Name

1e6d93a27b0d7e97df5405650986e32641696967c07df3fa8edd41063b49507b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1e6d93a27b0d7e97df5405650986e32641696967c07df3fa8edd41063b49507b']

Name

10686a12b7241a0836db6501a130ab67c7b38dbd583ccd39c9e655096695932e
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '10686a12b7241a0836db6501a130ab67c7b38dbd583ccd39c9e655096695932e']
Name
038187ceb4df706b13967d2a4bff9f67256ba9615c43196f307145a01729b3b8
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '038187ceb4df706b13967d2a4bff9f67256ba9615c43196f307145a01729b3b8']
Name
c27b64277c3d14b4c78f42ca9ee2438b602416f988f06cb1a3e026eab2425ffc
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'c27b64277c3d14b4c78f42ca9ee2438b602416f988f06cb1a3e026eab2425ffc']

Name
4e2c5513cf1c4a3c12c6e108d0120d57355b3411c30d59dfb0d263ad932b6868
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4e2c5513cf1c4a3c12c6e108d0120d57355b3411c30d59dfb0d263ad932b6868']

Name
192.3.152.183
Description
- **Zip Code:** N/A - **ISP:** ColoCrossing - **ASN:** 36352 - **Organization:** ColoCrossing - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** hml01.ficernera.info - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** New York - **City:** Buffalo - **Latitude:** 42.99 - **Longitude:** -78.73
Pattern Type
stix
Pattern

```
[ipv4-addr:value = '192.3.152.183']
```

Vulnerability

Name
CVE-2024-21887
Description
Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure contain a command injection vulnerability in the web components of these products, which can allow an authenticated administrator to send crafted requests to execute code on affected appliances. This vulnerability can be leveraged in conjunction with CVE-2023-46805, an authenticated bypass issue.
Name
CVE-2023-46805
Description
Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure gateways contain an authentication bypass vulnerability in the web component that allows an attacker to access restricted resources by bypassing control checks. This vulnerability can be leveraged in conjunction with CVE-2024-21887, a command injection vulnerability.

Malware

Name
Mirai

Attack-Pattern

Name
T1609
ID
T1609
Description
Adversaries may abuse a container administration service to execute commands within a container. A container administration service such as the Docker daemon, the Kubernetes API server, or the kubelet may allow remote management of containers within an environment.(Citation: Docker Daemon CLI)(Citation: Kubernetes API)(Citation: Kubernetes Kubelet) In Docker, adversaries may specify an entrypoint during container deployment that executes a script or command, or they may use a command such as `docker exec` to execute a command within a running container.(Citation: Docker Entrypoint)(Citation: Docker Exec) In Kubernetes, if an adversary has sufficient permissions, they may gain remote execution in a container in the cluster via interaction with the Kubernetes API server, the kubelet, or by running a command such as `kubectl exec`.(Citation: Kubectl Exec Get Shell)
Name
T1059
ID
T1059

Description
Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name
T1105

ID
T1105

Description
Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/

techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.(Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by [User Execution](https://attack.mitre.org/techniques/T1204) (typically after interacting with [Phishing](https://attack.mitre.org/techniques/T1566) lures).(Citation: T1105: Trellix_search-ms) Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

T1204

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary; running malicious JavaScript in their browser, allowing adversaries to [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539)s; or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204).(Citation: Talos

Roblox Scam 2023)(Citation: Krebs Discord Bookmarks 2023) For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name
T1190

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) or [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203). 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

T1082

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

StixFile

Value
f20da76d75c7966abcbc050dde259a2c85b331c80cce0d113bc976734b78d61d
d6f5fc248e4c8fc7a86a8193eb970fe9503f2766951a3e4b8c084684e423e917
cf1b85d4812f7ee052666276a184b481368f0c0c7a43e6d5df903535f466c5fd
b9d92f637996e981006173eb207734301ff69ded8f9c2a7f0c9b6d5fcc9063a2
b0bc9a42a874cab6583e4993de7cc11a2b8343a4453bda97b83b0c2975e7181d
a843971908aa31a81d96cc8383dcde7f386050c6e3437ad6a470f43dc2bf894b
9b5fe87aaa4f7ae1c375276bfe36bc862a150478db37450858bbfb3fb81123c2
8f0c5baaca3b81bdaf404de8e7dcca1e60b01505297d14d85fea36067c2a0f14
850d3521693b4e1ec79981b3232e87b0bc22af327300dfdc7ea1b7a7e97619cd
67d989388b188a817a4d006503e5350a1a2af7eb64006ec6ad6acc51e29fdcd5
5fcbe868a8c53b7146724d579ff82252f00d62049a75a04baa4476e300b42d15
5d155f86425b02e45a6a5d62eb8ce7827c9c43f3025bffd6d996aabd039d27f9
5b20ed646362a2c6cdc5ca0a79850c7d816248c7fd5f5203ce598a4acd509f6b

575f0acd67df2620378fb5bd8379fd2f2ba0539b614986d60e85822ba0e9aa08
53f6cedcf89fccdcb6b4b9c7c756f73be3e027645548ee7370fd3486840099c4
3e785100c227af58767f253e4dfe937b2aa755c363a1497099b63e3079209800
3d19de117388d50e5685d203683c2045881a92646c69ee6d4b99a71bf65dafa7
1e6d93a27b0d7e97df5405650986e32641696967c07df3fa8edd41063b49507b
10686a12b7241a0836db6501a130ab67c7b38dbd583ccd39c9e655096695932e
038187ceb4df706b13967d2a4bff9f67256ba9615c43196f307145a01729b3b8
c27b64277c3d14b4c78f42ca9ee2438b602416f988f06cb1a3e026eab2425ffc
4e2c5513cf1c4a3c12c6e108d0120d57355b3411c30d59dfb0d263ad932b6868

IPv4-Addr

Value
192.3.152.183

External References

- https://blogs.juniper.net/en-us/security/protecting-your-network-from-opportunistic-ivanti-pulse-secure-vulnerability-exploitation
- https://otx.alienvault.com/pulse/663de38e4eaac52e30197797