**Main Website vulnerability REPORT**

*Aaditya Singh Thakur 21BCY10236*

Website: <https://www.warframe.com/>

**Vulnerability Name: Host Fully Qualified Domain Name (FQDN) Resolution**

CWE: CWE-2009

OWASP Category: A1:2021 – Injection

Description: Host FQDN Resolution is a vulnerability that occurs when an attacker is able to resolve the FQDN of a remote host. This can be done by exploiting vulnerabilities in DNS servers, or by simply performing a reverse lookup on the IP address of the remote host.

Business Impact: Once an attacker knows the FQDN of a remote host, they can use this information to launch a variety of attacks, including:

* Phishing attacks: The attacker can send phishing emails to users that appear to be coming from a legitimate domain.
* Man-in-the-middle attacks: The attacker can intercept traffic between the user and the remote host, and impersonate either the user or the host.
* DNS cache poisoning attacks: The attacker can poison the DNS cache of the user's machine, causing it to resolve the FQDN of the remote host to a malicious IP address.

Vulnerability Path: Any application that accepts user input and then uses that input to resolve the FQDN of a remote host is at risk of this vulnerability. For example, a web application that allows users to search for products by name could be exploited if the application does not properly validate the user input.

Vulnerability Parameter: Any user-provided input that is used to resolve the FQDN of a remote host is a potential vulnerability parameter. For example, the following search query could be used to inject malicious DNS data:

product\_name=foo.com

Steps to Reproduce:

1. Identify an application that accepts user input and then uses that input to resolve the FQDN of a remote host.
2. Inject malicious data into the input field.
3. Observe the results.

Recommendation:

* Validate all user input before using it to resolve the FQDN of a remote host.
* Use a trusted DNS server.
* Implement a web application firewall (WAF).
* Keep application software up to date.

**Vulnerability Name: ICMP Timestamp Request Remote Date Disclosure**

CWE: CWE-2001

OWASP Category: M1:2021 – Insecure Cryptographic Storage

Description: ICMP Timestamp Request Remote Date Disclosure is a vulnerability that occurs when an attacker is able to send an ICMP timestamp request to a remote host and receive a response that includes the date and time set on the remote host. This information can be used by an attacker to defeat time-based authentication protocols.

Business Impact: Once an attacker knows the date and time set on a remote host, they can use this information to launch a variety of attacks, including:

* Brute-force attacks: The attacker can use the date and time information to guess the password for a time-based authentication protocol.
* Replay attacks: The attacker can record a legitimate authentication request and then replay it at a later time.
* Man-in-the-middle attacks: The attacker can intercept and modify the date and time information in an authentication request.

Vulnerability Path: Any system that responds to ICMP timestamp requests is at risk of this vulnerability. This includes most operating systems.

Vulnerability Parameter: The ICMP timestamp request message does not include any authentication information. This means that any attacker can send a timestamp request to any system.

Steps to Reproduce:

1. Send an ICMP timestamp request to a remote host.
2. Receive the ICMP timestamp response message.
3. Observe the date and time information in the response message.

Recommendation:

* Disable ICMP timestamp requests on all systems.
* Use a secure time synchronization protocol, such as NTP.
* Implement a firewall that blocks ICMP timestamp requests. Keep application software up to date.

**Vulnerability Name: TCP Port Scanning**

CWE: CWE-2000

OWASP Category: A1:2021 – Injection

Description: TCP Port Scanning is a vulnerability that occurs when an attacker is able to determine which TCP ports are open on a remote host. This can be done by sending SYN (synchronization) packets to the remote host and observing the response. If the remote host responds with a SYN/ACK (synchronization acknowledged) packet, then the port is open. If the remote host responds with an RST (reset) packet, then the port is closed.

Business Impact: Once an attacker knows which TCP ports are open on a remote host, they can use this information to launch a variety of attacks, including:

* Exploit known vulnerabilities in services running on open ports.
* Launch denial-of-service (DoS) attacks against open ports.
* Gain unauthorized access to the remote host.

Vulnerability Path: Any system that is accessible over TCP is at risk of this vulnerability.

Vulnerability Parameter: The TCP port number is the vulnerability parameter.

Steps to Reproduce:

1. Send a SYN packet to a remote host on a specific TCP port.
2. Observe the response from the remote host.
3. If the remote host responds with a SYN/ACK packet, then the port is open.
4. If the remote host responds with an RST packet, then the port is closed.

Recommendation:

* Use a firewall to block unauthorized access to TCP ports.
* Keep application software up to date.
* Use a network intrusion detection system (NIDS) to monitor for suspicious activity.

**Vulnerability Name: TCP/IP Timestamps Supported**

CWE: CWE-2009

OWASP Category: A1:2021 – Injection

Description: TCP/IP Timestamps Supported is a vulnerability that occurs when a remote host implements TCP timestamps. TCP timestamps are a feature that allows for more accurate round-trip time (RTT) measurements. However, a side effect of this feature is that the uptime of the remote host can sometimes be computed. This can be done by observing the difference between the timestamp values in the SYN and ACK packets.

Business Impact: Once an attacker knows the uptime of a remote host, they can use this information to launch a variety of attacks, including:

* Determine the patch level of the remote host.
* Launch timing-based attacks.
* Correlate information from multiple sources.

Vulnerability Path: Any system that implements TCP timestamps is at risk of this vulnerability.

Vulnerability Parameter: The TCP timestamps option is the vulnerability parameter.

Steps to Reproduce:

1. Send a SYN packet to a remote host with the TCP timestamps option enabled.
2. Receive the SYN/ACK packet from the remote host.
3. Observe the timestamp values in the SYN and ACK packets.
4. Calculate the difference between the timestamp values.
5. Use the difference in timestamp values to estimate the uptime of the remote host.

Recommendation:

* Disable TCP timestamps on all systems.
* Use a firewall to block access to the TCP timestamps option.
* Keep application software up to date.

**Vulnerability Name: Traceroute Information Disclosure**

CWE: CWE-2009

OWASP Category: A2:2021 – Sensitive Data Exposure

Description: Traceroute Information Disclosure is a vulnerability that occurs when an attacker is able to obtain traceroute information for a remote host. Traceroute information can be used to identify the network path between the attacker and the remote host. This information can be used by attackers to launch a variety of attacks, including:

* Mapping the network topology of an organization.
* Identifying potential targets for attack.
* Launching denial-of-service (DoS) attacks.

Business Impact: Once an attacker has obtained traceroute information for a remote host, they can use this information to launch a variety of attacks that can disrupt or disable business operations.

Vulnerability Path: Any system that responds to traceroute requests is at risk of this vulnerability.

Vulnerability Parameter: The traceroute request message does not include any authentication information. This means that any attacker can send a traceroute request to any system. Steps to Reproduce:

1. Send a traceroute request to a remote host.
2. Receive the traceroute response message.
3. Observe the network path information in the response message.

Recommendation:

* Disable traceroute on all systems.
* Use a firewall to block traceroute requests.
* Keep application software up to date.