radware

ERT Threat Alert
Jenkins Denial-of-Service Attacks
February 10, 2020

Executive Summary

Radware's threat research has surveyed the cybersecurity landscape related to Jenkins Security Advisory 1641, also known as CVE-2020-2100, and confirm that over 12,000 exposed Jenkins' servers can easily be abused by an attacker to launch distributed reflective denial-of-service (DrDoS) attacks with an average amplification factor of 3.00. Exposed Jenkins servers are under an immediate threat of infinity reply loops between each other. That loop can be initiated by a remote attacker using a single, spoofed UDP packet.

Background

On January 29, 2020, the Jenkins project published a security advisory[1] containing a vulnerability with UDP amplification reflection attack potential. Security alert 1641, also known as CVE-2020-2100, reports the vulnerability discovered by Adam Thorn from the University of Cambridge and how it impacts Jenkins versions 2.218 and earlier as well as LTS 2.204.1 and earlier.

Jenkins, by default, supports two network discovery services: UDP multicast/broadcast and DNS multicast. The vulnerability allows attackers to abuse Jenkins servers by reflecting UDP requests off port UDP/33848, resulting in an amplified DDoS attack containing Jenkins metadata. This is possible because Jenkins/Hudson servers do not properly monitor network traffic and are left open to discover other Jenkins/Hudson instances. Jenkins/Hudson responds to any traffic on UDP port 33848. An attacker can either send a UDP broadcast packet locally to 255.255.255.255:33848 or they could send a UDP multicast packet to JENKINS_REFLECTOR:33848. When a packet is received, regardless of the payload, Jenkins/Hudson will send an XML response of Jenkins metadata in a datagram to the requesting client, giving attackers the ability to abuse its UDP multicast/broadcast service to carry out DDoS attacks.

Carefully crafted UDP packets can also make two Jenkins servers go into an infinite loop of replies, causing a denial of service against both servers. When exposed on the internet, port UDP/33848 becomes a public threat and can be abused for DrDoS or leveraged to take out multiple Jenkins clusters.

The vulnerability was fixed in Jenkins 2.219 and LTS 2.204.2 by disabling both UDP multicast/broadcast and DNS multicast by default. Administrators can reenable those features, but Radware advises ensuring those services are not exposed to the public internet.

Amplification DoS Attack

By crafting UDP packets with a victim's IP as the source and the IP of an exposed Jenkins server and port UDP/33848 as the destination, a malicious actor can create a reflective flood of packets between the Jenkins server and the victim (see Figure 1). The reflective flood will benefit from an amplification factor that varies between Jenkins servers, but on average provides a 3.00 amplification ratio.

[1] https://jenkins.io/security/advisory/2020-01-29/

IP		Port	
SRC	DST	SRC	DST
Victim	Jenkins 1	XXXX	33848

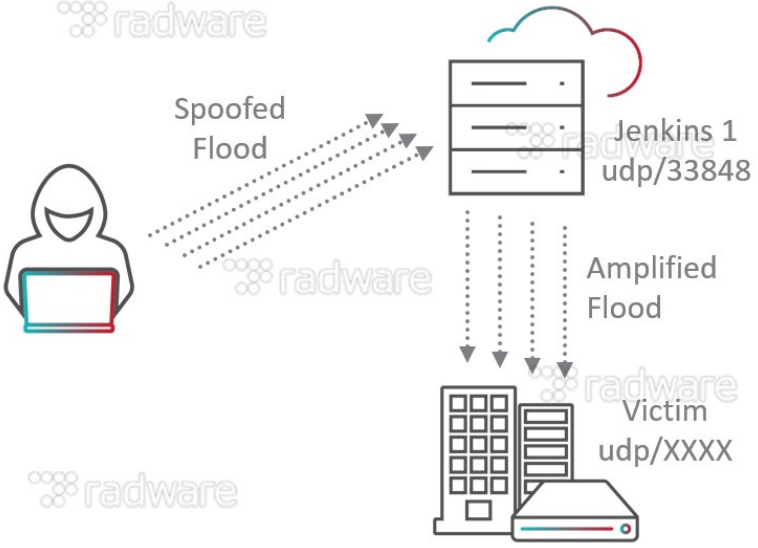

Figure 1: Amplification DoS using Jenkins

Radware research verified and confirmed the ability to leverage exposed Jenkins servers in attacks against random victims and ports.

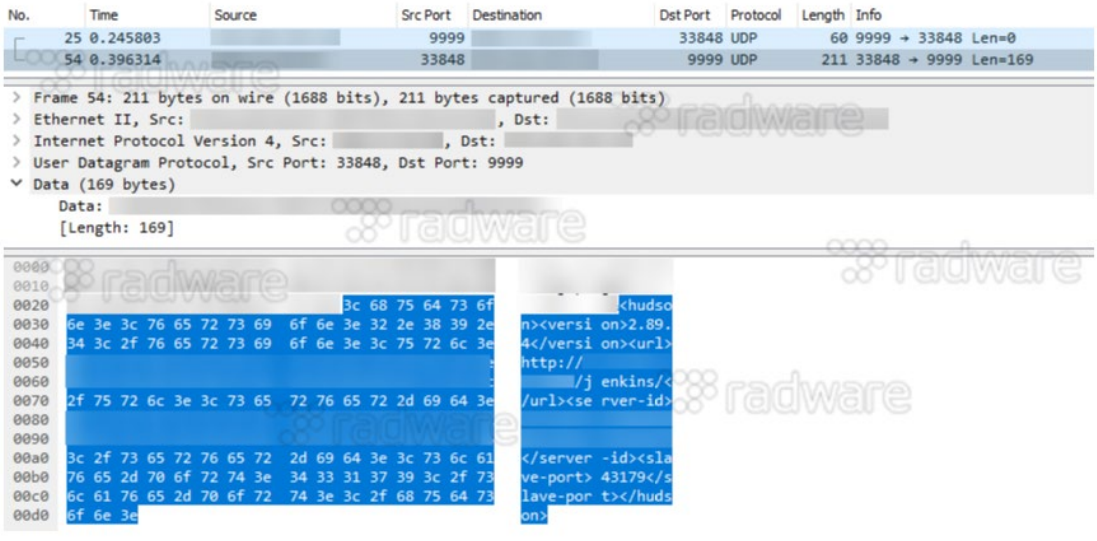

Figure 2: Spoofed UDP packet from port 9999 to an internet exposed Jenkins server

Figure 2 illustrates a spoofed UDP packet which sends a request from port 9999 to an exposed Jenkins server on port 33848. The smallest request has a packet size of 60 bytes. In this case, the server responds with a packet of 211 bytes. The response will depend on the server URL and service ID settings as well as optional attributes, such as the slave-port.

Infinity Reply Loop

The Jenkins discovery service responds to any request, independent of the contents of the request. By consequence, a carefully crafted packet can initiate a reply loop between two Jenkins servers.
By crafting a UDP packet using the source IP of an exposed server and the destination IP of another exposed Jenkins server (both source and destination set to the Jenkins discovery service UDP/33848 port), both Jenkins servers will go into an infinite reply loop.

In Figure 3, a crafted packet is sent to the exposed server (Jenkins 1) with a spoofed source IP and port of another exposed server (Jenkins 2). Jenkins 1 will respond to the crafted request with a new UDP packet containing the service location information and send it to the source IP and port of the crafted request packet. This results in a UDP packet from Jenkins 1 to Jenkins 2. Jenkins 2 will interpret the UDP packet from Jenkins 1 as a request, ignoring whatever payload the packet carries. Jenkins 2 will respond with a new UDP packet to Jenkins 1 port 33848.

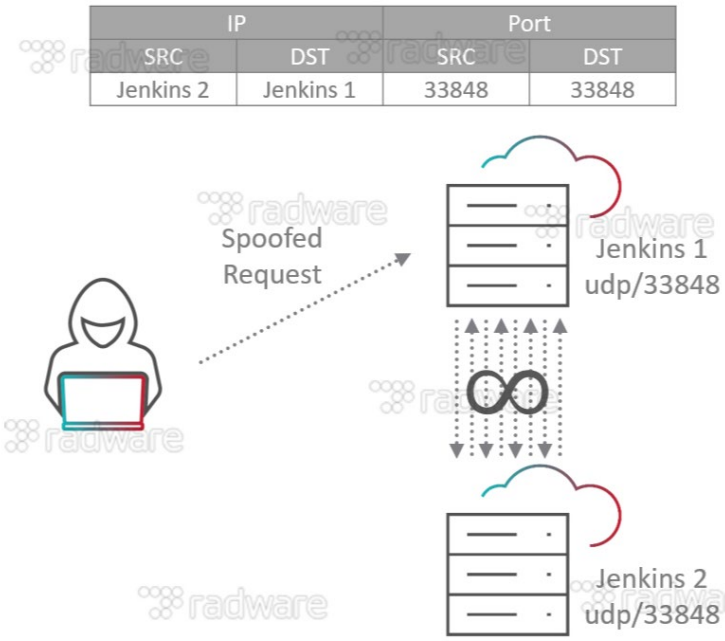

Figure 3: Initiating an infinite reply loop between two Jenkins servers

Radware research verified and confirmed the ability to initiate reply loops between publicly exposed Jenkins servers, independent of their location. Figure 4 contains the packet capture of a request packet generated from a test host, containing actual information from an exposed Jenkins server directed to a second exposed Jenkins server. The second packet is the response from the second server to the originating server. The packet sizes remain identical between replies and depend on the responding server.

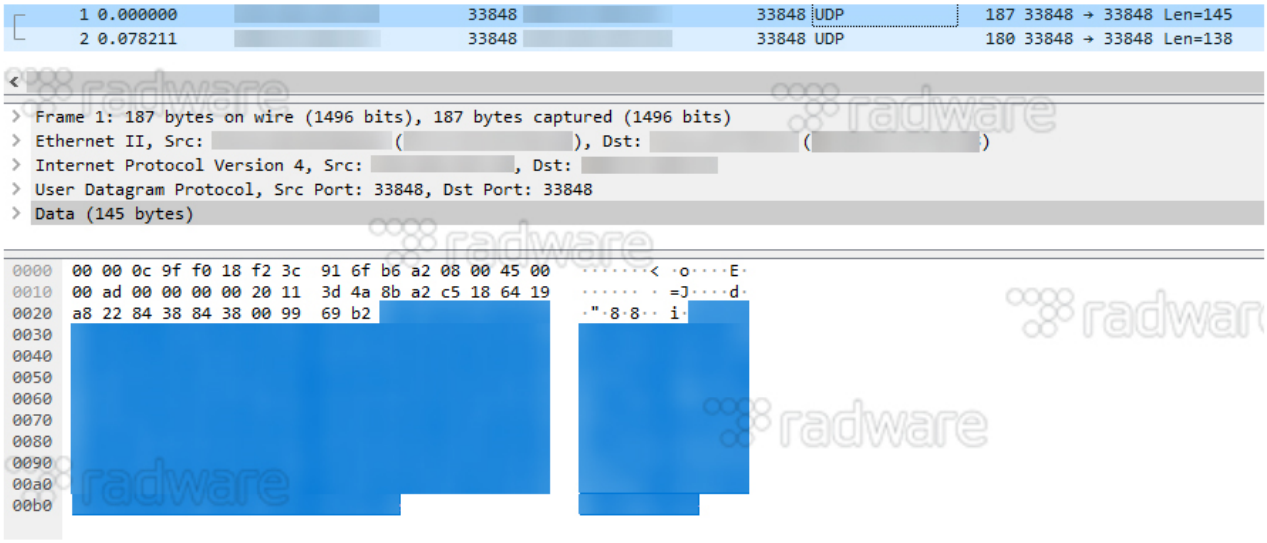

Figure 4: Packet capture of request and response cycle in infinite reply loop between two Jenkins servers

A malicious actor would be able to create multiple infinite reply loops between a random batch of exposed Jenkins servers on the internet, eventually causing a fully meshed, mutual, and infinite stream of packets between the exposed internet hosts.

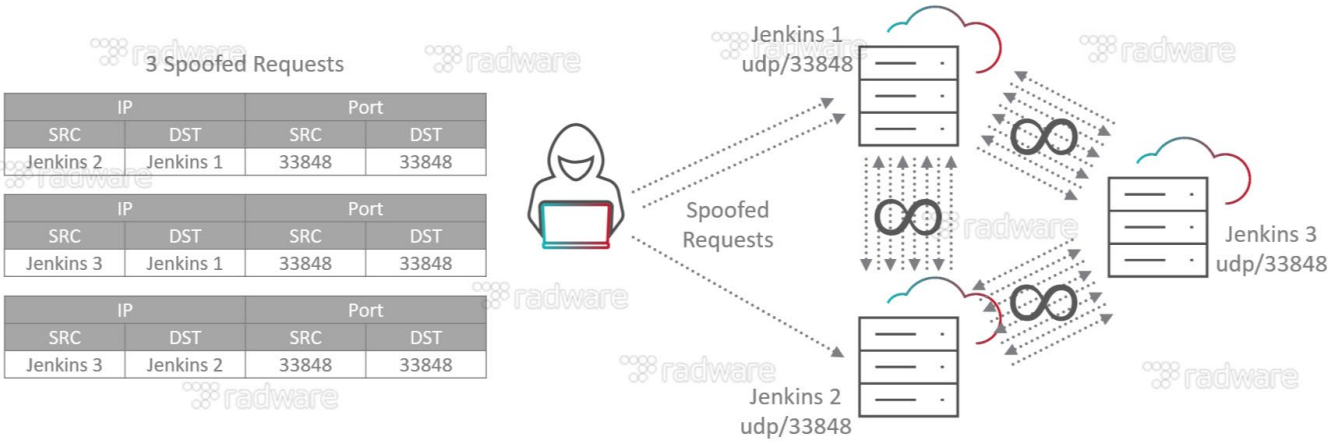

Figure 5: Initiating a fully meshed infinite reply loop between three exposed servers

Given the total number of exposed servers discovered by our researchers, a fully meshed denial-of-service attack of 12,000 exposed Jenkins servers would be possible using n x (n – 1) / 2 spoofed requests.

Threat Landscape for CVE-2020-2100

Last week, following the Jenkins Security Advisory, Radware's researchers began scanning the internet for Jenkins servers vulnerable to CVE-2020-2100. Recently, there have been several UDP amplification methods disclosed. Our researchers wanted to know if and how many servers were exposed to assess the risk of this new attack vector.

A responsible internet scan, respecting exclusion ranges as provided by Masscan[2] author Robert Graham, revealed IP addresses with port UDP/33848 open. Of those, 12,802 responded to a Jenkins discovery request. Exposed Jenkins servers are distributed across the globe, but have a major presence in Asia, Europe and North America.

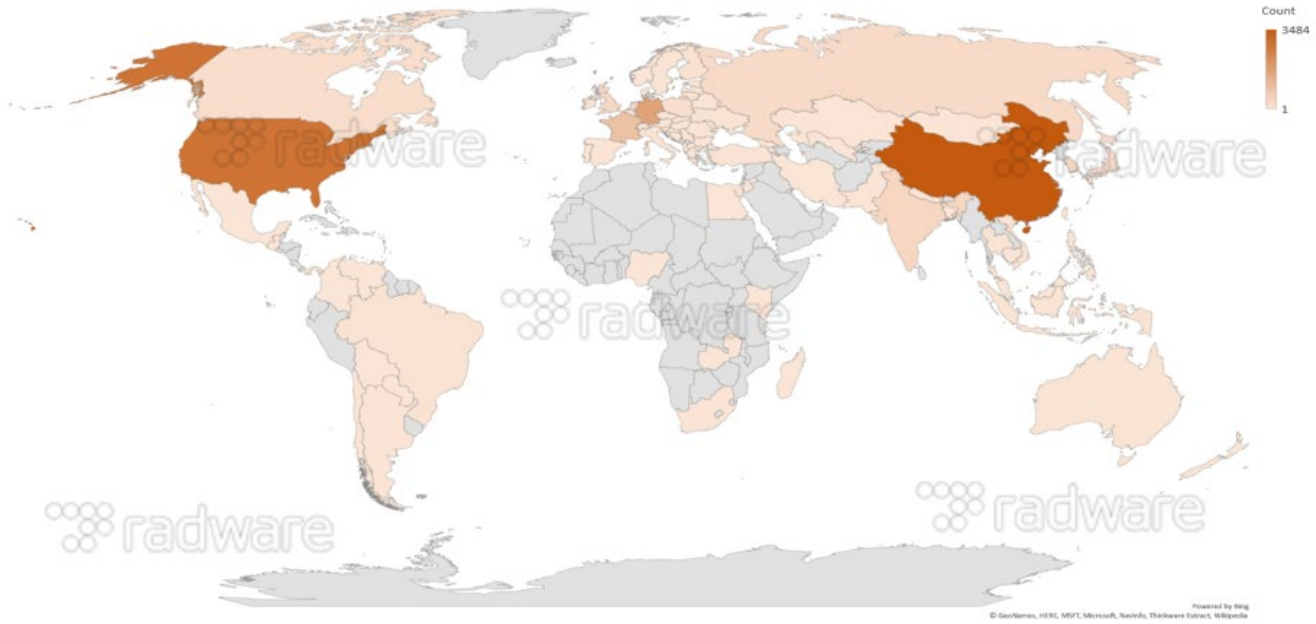

Figure 6: Geographic spread of exposed Jenkins servers

Reflection and Amplification

After gathering the Jenkins' amplification list, we began testing the exposed servers for reflective and amplification properties. Jenkins Security Advisory 1641 reported that the UDP multicast/broadcast service used by Jenkins could be leveraged in an amplification reflection attack. They reported that a single byte request to this service would respond with more than 100-bytes of Jenkins metadata. Once we began analyzing the server replies, we started to understand the level of risk presented by this new amplified attack vector. A server reply to an empty request, 28 bytes, generates an amplification factor between 1.87 and 4.65, depending on the server. Radware's research was able to determine the average bandwidth amplification factor (BAF) for the Jenkins reflective amplification attack, across all currently exposed servers, as being 3.00.

Summary:	
Exposed servers:	12802
Max amp Ratio:	4.65
Min amp Ratio:	1.87
Avg amp Ratio:	3.00

Figure 7: Jenkins BAF landscape

[2] https://github.com/robertdavidgraham/masscan/blob/master/README.md

Reasons for Concern and Recommendations

DDoS Tactics Techniques and Procedures (TTP) have been evolving over the last year. In 2019, we saw three new vectors used to launch reflective amplified attacks. ARMS[3] abuses Apple's Remote Desktop feature on port 3283 to create a BAF of 35. We also saw the widespread use of Web Service Dynamic Discovery[4] (WS-Discovery), a protocol used by hundreds of thousands of devices to launch reflective amplified attacks. Attackers can leverage WS-Discovery for amplification by reflecting attack traffic off of port 3702 for a BAF ranging between 10 and 100. At the end of 2019, we also saw attackers leverage TCP handshakes for a reflective attack that gained amplification through retransmission.[5]

As predicted, the resurgence in DDoS attack vectors will continue to grow into 2020 as botnet development plateaus. We now have our first confirmed amplification attack vector of the year. CVE-2020-2100 possess a BAF ranging between 1.87 and 4.65. Combined with over 12,000 exposed Jenkins servers globally, it creates a viable DDoS threat.

For owners of exposed Jenkins servers, this is an imminent denial-of-service threat. A remote malicious actor can initiate infinite reply loops through carefully crafted UDP packets. Those owners should take immediate action to limit the public access to their Jenkins servers and update their Jenkins clusters as soon as possible to at least Jenkins version 2.219 or LTS 2.204.2. These versions disable both UDP multicast/broadcast and DNS multicast by default. If there is a need for auto-discovery of Jenkins instances, administrators can reenable both features, however do so responsibly by ensuring those services are not exposed to the public internet.

CVE-2020-2100

Jenkins 2.218 and earlier, LTS 2.204.1 and earlier are vulnerable to a UDP amplification reflection denial-of-service attack on port 33848.[6]

IOCs

Attack traffic originating from UDP/33848 with an XML payload structure like Figure 10.

```
<hudson>
  <version>1.354</version><!-- version of the Jenkins -->
  <url>http://server/hudson/</url><!-- the top page of the Jenkins -->
  <slave-port>12345</slave-port><!-- TCP port number for slaves and CLIs to connect to -->
  ... more elements may appear here ...
</hudson>
```

Figure 8: Jenkins UDP multicast/broadcast message structure[7]

[3] https://www.zdnet.com/article/macos-systems-abused-in-ddos-attacks/
[4] https://www.zdnet.com/article/protocol-used-by-630000-devices-can-be-abused-for-devastating-ddos-attacks/
[5] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/tcp-reflection-attacks/
[6] https://nvd.nist.gov/vuln/detail/CVE-2020-2100
[7] https://wiki.jenkins.io/display/JENKINS/Auto-discovering+Jenkins+on+the+network

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.