Application Server Security Report

Period: 2016-06-01 to 2016-07-20

Generated At: 2016-07-21 17:18:07

Application Server Domain/IP: Total

Purpose

1. Help to find risk quickly and provide information such as attack source, target, impact and solutions.

Contents

1. Current security state and trend of the entire network
2. Application servers prone to critical or high-risk vulnerabilities or attacks
3. Solutions to existing issues

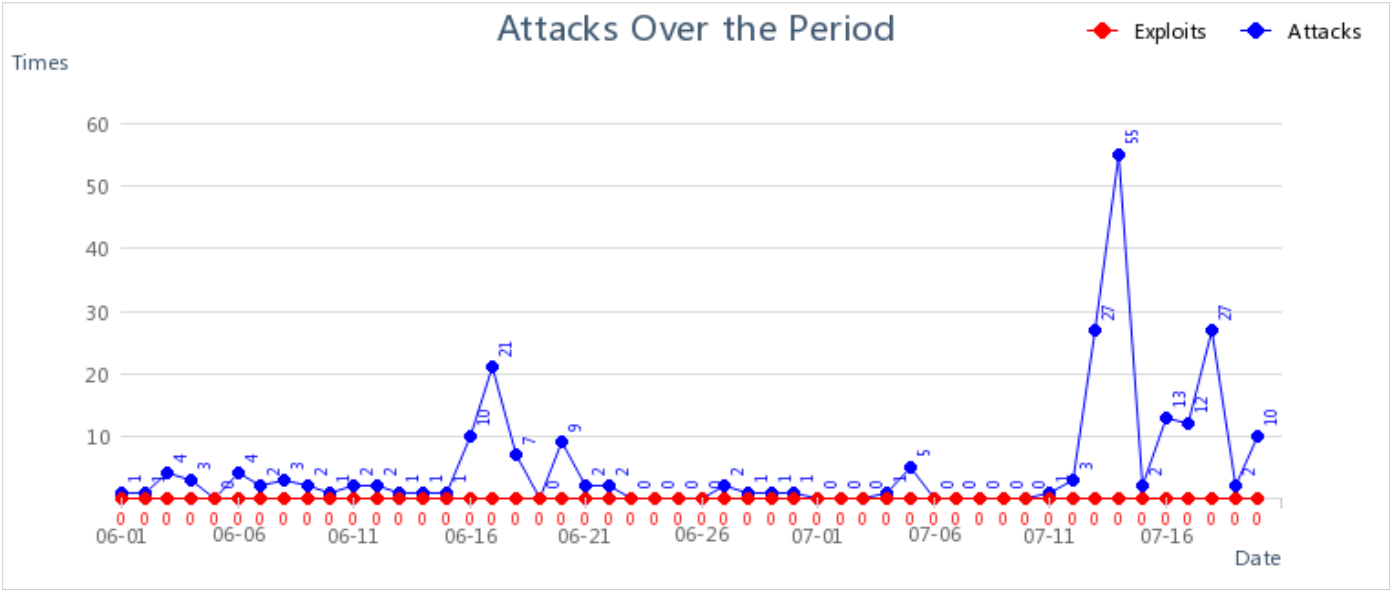
Security Overview

Summary

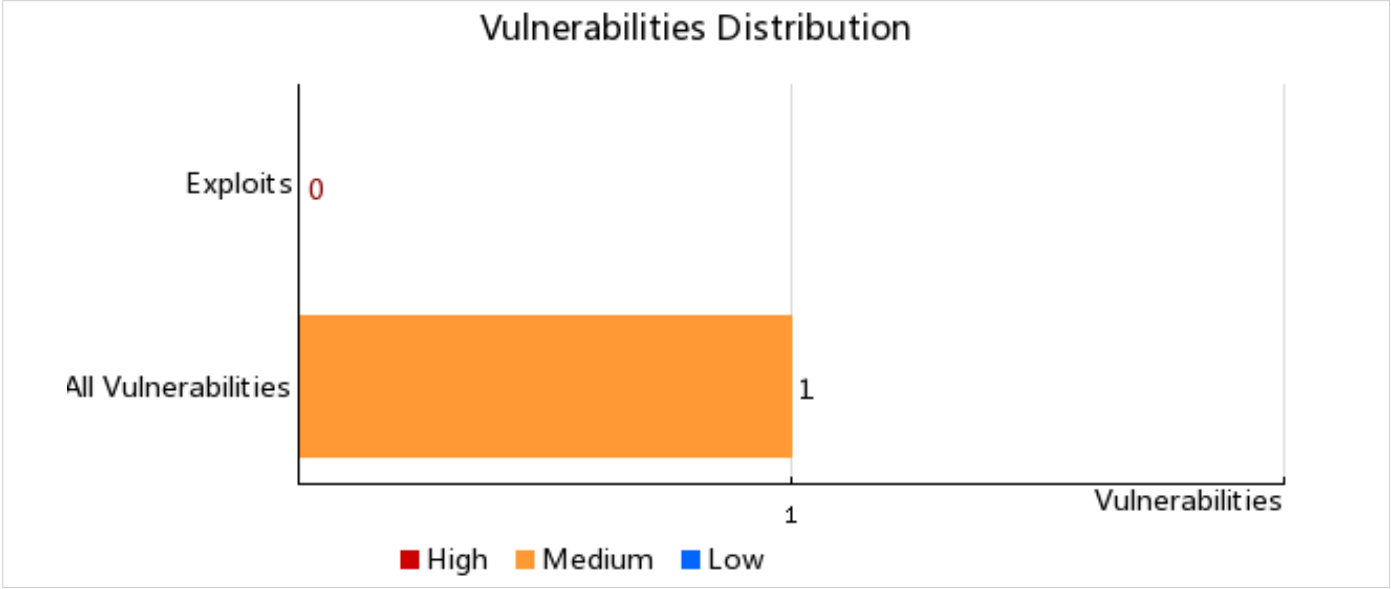
2016-06-01 to 2016-07-20, overall security rating is Fair, (see Security Rating Regulations).

After checking security of application servers based on Layer 2 to Layer 7 analysis, vulnerability analysis, License Detection, we found 1 Rule Database Expired, 0 high-risk vulnerabilities, average number of attacks each day is less than 100. Vulnerable targets are 192.168.20.100, 10.1.1.2, 122.155.21.250 Application Server Domain/IP,Application servers are undergoing few attacks, and the current protection policy can shield them away from eventual attack.

Attack possibility over the past period is as follows:
The more attacks, the worse the network security. The more exploits, the more likely the network will be intruded by attacker. Using next-generation firewall can protect the system against exploits and attacks by attackers. An exploit may be a piece of software that takes advantage of a bug or vulnerability in order to cause unintended behavior to computer software. And it's the attack that can be exploited by attackers, such as denial-of-service attack.



Vulnerability Distribution:
2016-06-01 to 2016-07-20, 1; for medium-risk vulnerability, there are 1.



Security Rating

Security Rating Based on Attack

No.	Attack Type	Description	Attacks Per Day	Security Level
1	Application Server Security	Exploited but protected now	4	Good

Security Rating Based on Vulnerability

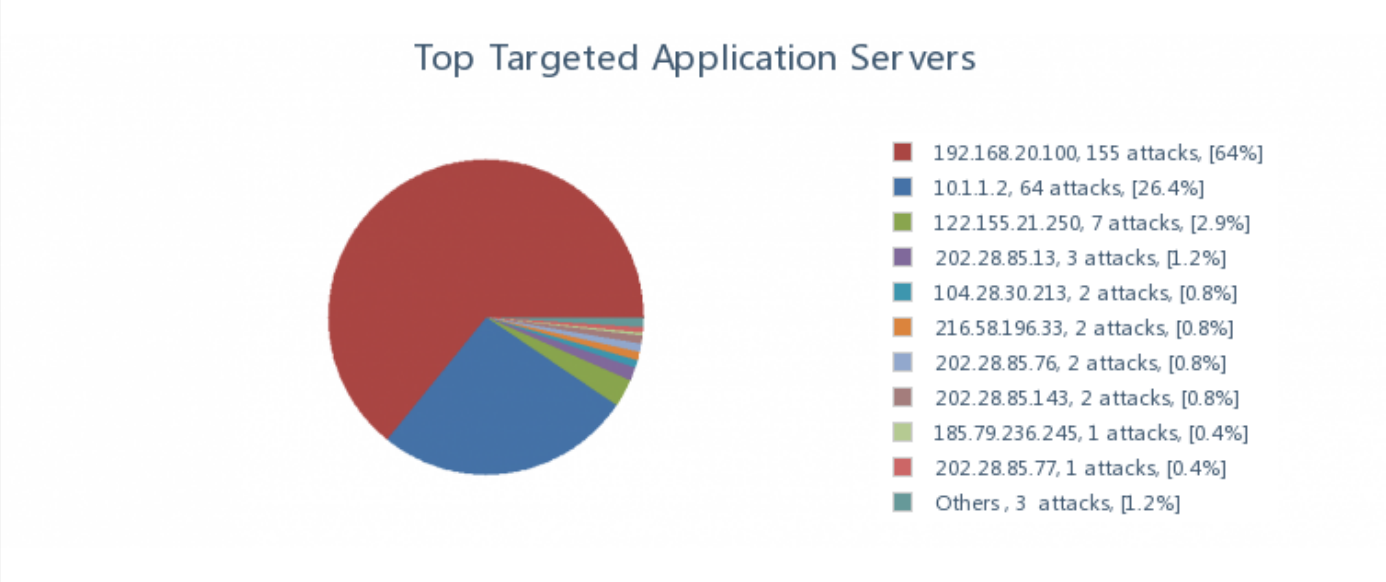
No.	Vulnerability Type	Description	High-Risk Vulnerabilities	Security Level
1	All Vulnerabilities	Potential risk	0	Excellent

Security rating is based on rule event:

No.	Type	Description	Count	Security Level
1	Rule Database Detection	Anti-Virus Database Rule Database Expired	1	Fair

Application Server Security

Application server 192.168.20.100 accounts for 64.05%, 10.1.1.2 accounts for 26.45%, 122.155.21.250 accounts for 2.89%, The higher the threat level, the more vulnerable the server is, and the higher threat the server is facing.



Attack Analysis

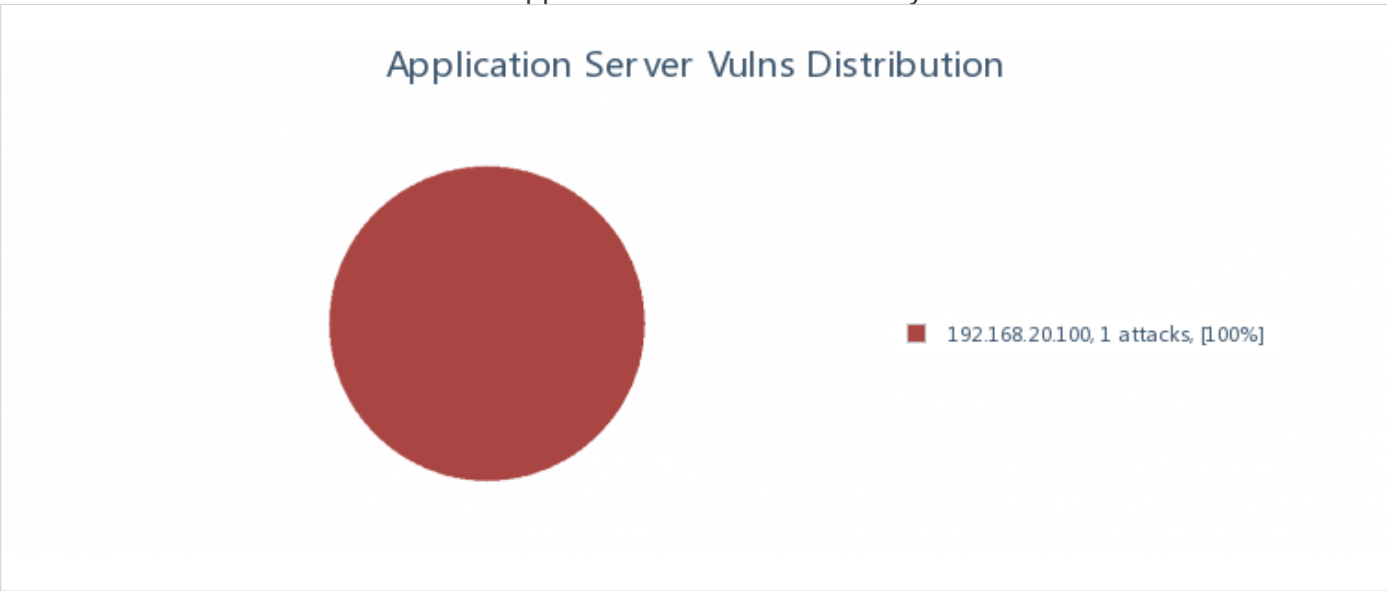
Top Targeted Application Servers

No.	Application Server	Attack Type	Attack Count	Percent	Exploits	Threat Level
1	192.168.20.100	Request method filter(76), Brute-force attack(68), Port scan(11)	155	64.05%	0	High
2	10.1.1.2	Port scan(63), UDP flooding attack(1)	64	26.45%	0	High
3	122.155.21.250	UDP flooding attack(7)	7	2.89%	0	High
4	202.28.85.13	UDP flooding attack(3)	3	1.24%	0	High

5	104.28.30.213	Application Vulnera-bility(2)	2	0.83%	0	High
6	216.58.196.33	UDP flooding attack(2)	2	0.83%	0	High
7	202.28.85.76	UDP flooding attack(2)	2	0.83%	0	High
8	202.28.85.143	UDP flooding attack(2)	2	0.83%	0	High
9	185.79.236.245	UDP flooding attack(1)	1	0.41%	0	High
10	202.28.85.77	UDP flooding attack(1)	1	0.41%	0	High
11	Other hosts		3	1.2%		

Vulnerability Assessment

192.168.20.100 are the most vulnerable application servers. Vulnerability distribution is as follows:



Most Vulnerable Application Servers

No.	Application Server	Vulnerability Type	Vulnerability Count	Exploits	Threat Level
1	192.168.20.100	Wrong Configuration(1)	1	0	Medium

Analysis Based on Risk Type

Based on analysis on traffic from several aspects, we found 6 categories of applications are in security threat. For those at high threat level, there are 3. For those at medium threat level, there are 3, which are as follows:

Application Server Security - Attack Types

No.	Attack Type	Attack Count	Percent	Exploited?	Threat Level
1	Brute-force attack	68	28.1%	No	High
2	UDP flooding attack	22	9.1%	No	High
3	Application Vulnerability	2	0.8%	No	High
4	Request method filter	76	31.4%	No	Medium
5	Port scan	74	30.6%	No	Medium

Application Server Security - Top Vulnerability Types

No.	Name	Vulnerability Count	Target IP	Threat Level
1	Wrong Configuration	1	-	Medium

Analysis Based on Specific Attack

Brute-force Attack

Description

Open password authentication service server, an attacker can use brute force tool for servers. once a successful brute force, the attacker can do anything through the server.

Target Server

Brute-force attack: 68 attacks, which are as follows:

No.	Target Domain/IP	Details	Attack Count
1	192.168.20.100	-	68

Solution

1.Try to limit the server only allows network users to access.
2.Change the password for the special characters plus numbers plus characters at least 8 characters mixing.
3.Open IPS turned brute tactics and select block.

UDP Flooding Attack

Description

DDoS, Distributed Deny of Service in short, is an attack that attacker sends immense error data packets or partially connected packets to target server, with the purpose of consuming all the bandwidth and allowed connections, CPU and memory resources of the server, so that the server cannot provide services to legitimate users properly.

Target Server

UDP flooding attack: 22 attacks, which are as follows:

No.	Target Domain/IP	Details	Attack Count

1	122.155.21.250	-	7
2	202.28.85.13	-	3
3	216.58.196.33	-	2
4	202.28.85.76	-	2
5	202.28.85.143	-	2
6	202.28.85.77	-	1
7	10.1.1.2	-	1
8	172.217.25.1	-	1
9	172.217.24.225	-	1
10	185.79.236.245	-	1
11	Other hosts	-	1

Solution
1.Enable anti-DDoS attacks, both inside and outside DDoS attack, and configure the corresponding policy.

Application Vulnerability

Description
Attacker takes advantage of the vulnerabilities in various application software (such as IM, P2P download tool, medial player, games, security and backup software) to disconnect client from Internet, which exits subsequently because of error. User then needs to reinstall the software to get availability again.

Target Server
Application Vulnerability: 2 attacks, which are as follows:

No.	Target Domain/IP	Details	Attack Count
1	104.28.30.213	-	2

Solution
1.Install application program SP to fix the vulnerabilities.
2.Enable firewall IPS, configure and enable IPS rule to protect the corresponding hosts.

Request Method Filter

Description
Attacker takes advantage of the vulnerability to download files from Web server, upload malicious file or remove any file without logging in to the Web server.

Target Server
Request method filter: 76 attacks, which are as follows:

No.	Target Domain/IP	Details	Attack Count
1	192.168.20.100	**Dst Name:** http://rtsp://202.29.105.31:3454/Media/Live/Normal?camera=C_1&streamindex=2	76

Solution
1.Disable unnecessary HTTP methods, including the method for defining WEBDAV.

Port Scan

Description
DDoS, Distributed Deny of Service in short, is an attack that attacker sends immense error data packets or p-artially connected packets to target server, with the purpose of consuming all the bandwidth and allowed c-onnections, CPU and memory resources of the server, so that the server cannot provide services to legitimate users properly.

Target Server
Port scan: 74 attacks, which are as follows:

No.	Target Domain/IP	Details	Attack Count
1	10.1.1.2	-	63
2	192.168.20.100	-	11

Solution
1.Enable anti-DDoS attacks, both inside and outside DDoS attack, and configure the corresponding policy.

Analysis Based on Specific Vulnerability

Wrong Configuration

Description
Wrong configuration or security vulnerability of Web server often makes information disclosed to the Inter-net. System files or configuration files are vulnerable to leakage, making sensitive information available to I-nternet users, such as username, password, source code, server information, configuration, internal IP addre-ss, email address, etc.

Target Server
Wrong Configuration: 1, which are as follows:

No.	Target Domain/IP	Count
1	192.168.20.100	1

Solution
1.Webmaster changes the settings to not show user the returned error information.
2.Use Web Application Firewall(WAF).

Security Rating

Excellent

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, no high-risk vulnerability is found. Threat does not affect application server security and user access right assignment. Critical security issue will not occur at present.

Good

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, less than 10 high-risk vulnerabilities are found. Average number of attacks each day is less than 100. Application server and user are undergoing few attacks, and the current protection policy can shield them away from eventual attack.

Fair

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, 10 - 50 high-risk vulnerabilities are found. Average number of attacks each day is between 100 and 1000. Application server and user are undergoing some attacks, and the current protection policy can shield them away from eventual attack.

Poor

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, more than 50 high-risk vulnerabilities are found. Average number of attacks each day is more than 1000. Application server and user are undergoing a lot attacks, or even APT(Advanced Persistent Threat) attack. Urgent protection is needed and vulnerability must be fixed.

Remarks

When the device detects that license gets invalid, expired or the rule database license gets expired, the security rating will de degraded one rank; while APT or WebShell attack is detected, the security rating becomes critical.

Description

Current Software Version: AF6.8.232 EN Build20160328

Current Database Version:

No.	Name	Current Version Released
1	Anti-Virus Database	20160627 18:00:00
2	URL Database	20160711 09:00:00
3	Vulnerability Database	20160714 17:00:00
4	Software Update	20160517 17:16:29
5	Application Ident Database	20160530 12:34:56
6	WAF Signature Database	20160630 17:00:00
7	Data Leak Protection	20160627 09:39:55
8	Malware Signature Database	20160715 09:22:22
9	Vulnerability Analysis Rule	20160706 17:00:00
10	Malicious Connection Database	20160715 10:50:12
11	Threat Intelligence Database	20160718 16:30:01