DOS attack on www_server from multiple IP addresses

- **Product:** Aleph
- **Product Version:** 20, 21, 22, 23
- **Relevant for Installation Type:** Dedicated-Direct, Direct, Local, Total Care

Description

Our system is very slow and OPAC users are seeing the message: "The requested file was not found on the server. Please contact the library administration and inform them about this problem "

The following message is appearing in the www_server log: "Error: License limit exceeded", and we see the following "HeyAlephIgnoreThis" search coming from about 100 different IP addresses:

```
request: "/F/?func=find-
d&local_base=XXX01PUB&find_code=ISBN&HeyAlephIgnoreThis01=9780415428668&request=9780415428668&adjacent1=N&
_code=WRD&HeyAlephIgnoreThis02=&request=&adjacent2=N&find_code=WRD&HeyAlephIgnoreThis03=&request=&adjacent
filter_code_1=WLN&filter_code_2=WYR&filter_code_3=WYR&filter_code_4=WTP&filter_code_5=WSC&filter_request_2
lter_request_3=&filter_request_5=&filter_request_4=BK&filter_request_1="
```

This seems like a DOS (Denial of Service) attack? How can we stop it?

Resolution

The "License limit exceeded" message is discussed, generally, in the article "Opac not accessible, error 'License limit exceeded' ". The case where the attack is coming from multiple IP addresses is more complicated. There can be various ways (botnets, compromised PC's, etc.) that an attacker can generate transactions from different IP addresses.

In most cases, if there are 100,000 transactions, they won't be coming from 100,000 IP addresses, but certain IP addresses will have large numbers. The following SQL can be used to determine what IP addresses the most transactions are coming from:

```
> s+ vir01
vir01@ALEPH23> select Z63_CLIENT_ADDRESS, count(*) from z63 group by
Z63_CLIENT_ADDRESS order by count(*) asc;
```

IP addresses with hundreds of z63 (session) records are probably not normal activity. You can try blocking these individually with the firewall or server_ip_allowed, as described in the general article.

But there may be too many for this to be practical. What one site did, as a temporary measure, was to create a list of allowed IP addresses -- basically some campus IP address ranges -- and to deny other IP addresses. This is what that would look like in server_ip_allowed:

```
W A 123.456.789.*
```

```
W A 657.43.235.*
<etc.>
```

(Note: There no need for a "`W D *.*.*.*`" line. See Additional Information below.)

The disadvantage to this is, of course, that legitimate off-campus users will be denied access.

Jira Issue SEC-238 was closed by the Ex Libris Security Team with this comment: "Ex Libris recommends that customers consult with their internal security group. Denial of service attacks (DOS) first and foremost are prevented by firewalls, including Web Application Firewalls."

One site added a

```
RewriteCond ...

RewriteRule ...
```

containing a distinctive element of the request string the attacker was using to their ./apache/conf/httpd.conf file. This succeeded in blocking the vast majority of the transactions. Contact jerry.specht@exlibrisgroup.com for more information.

Additional Information

Note: **The default is for IP addresses to be denied unless they are specifically allowed.** The "D" is used in a case where you want to allow all IP addresses except a few, such as:

```
W D 352.43.235.*

W D 957.4.37.*

W A *.*.*.*
```

- **Article last edited:** 12-Mar-2017