**System software and applications not updated**

**SEVERITY: MODERATE HIGH**

**VULN. CODE:** SSAP-NU

**AUTH. REQUIRED:**

**VULNERABILITY DESCRIPTION**

Keeping the system and application software up-to date is a fundamental practice in the management of the systems and the applications in order to keep a high standard of corporate security. The missing updates or the missing security patches and/or workarounds, grants the exposure for a long period of time of the systems and the applications to public domains vulnerabilities and it highly reduces the effort that a generic threat agent has to make to carry out a successful attack. During the course of the analysis activities, we found out that some system components and/or application ones are not updated to the latest version made available by the vendor. We highlight that the following vulnerabilities could be exploited from a threat agent in order to carry out a successful attack with the aim to either access the information kept in the system, either to do a denial of service or to compromise the systems.

The following outdated and vulnerable software applications were detected:

* **SoftwareName   
  Version:** 2.4.29 **Host:** 104.214.239.16 **Severity: HIGH** (CVE-2019-0211) **CVE:** CVE-2017-15710…  
    
  The next Box shows the evidence of the software component version in the response header.

|  |
| --- |
| **Response: https://10.72.16.13:2224/**  HTTP/1.1 200 OK  Content-Type: text/html;charset=utf-8  Content-Length: 20  X-Xss-Protection: 1; mode=block  X-Content-Type-Options: nosniff  X-Frame-Options: SAMEORIGIN  Server: WEBrick/1.3.1 (Ruby/2.0.0/2015-12-16) OpenSSL/1.0.2k  Date: Mon, 19 Oct 2020 10:50:40 GMT  Connection: close  Set-Cookie: rack.session=5a1dcd7d2325a2bea4788741076243f22cc4f9de8266f041c34a6d2d4e0b13cd; path=/; expires=Mon, 19 Oct 2020 11:50:40 -0000; secure; HttpOnly |

**Box 1 – Leak software version: not updated**

**SUGGESTED SOLUTIONS**

It is suggested to first adopt countermeasures on the perimeter defense systems in order to mitigate the exploitation of the vulnerabilities carried by a generic threat agent by blocking the requests specifically made to exploit the vulnerabilities or by neutralizing the values supplied to the vulnerable application components. After applying the suggested workaround and after checking out the release notes from the vendors, it is suggested to update the system software and the application software that provide the services to the latest version available.

**REFERENCES**

More information regarding the vulnerability and its possible solutions can be found on the following addresses:

**REF 1 – https://www.cvedetails.com/**