CVE-2019-3929

1 - Caracterização do CVE escolhido na semana #2:

* Identificação: descrição geral da vulnerabilidade, incluindo aplicações/sistemas operativos relevantes (max 4 itens com 20 palavras cada)
* Catalogação: o que se sabe sobre o seu reporting, quem, quando, como, bug-bounty, nível de gravidade, etc. (max 4 itens com 20 palavras cada)
* Exploit: descrever que tipo de exploit é conhecido e que tipo de automação existe, e.g., no Metasploit (max 4 itens com 20 palavras cada)
* Ataques: descrever relatos de utilização desta vulnerabilidade para ataques bem sucedidos e/ou potencial para causar danos (max 4 itens com 20 palavras cada)

2 - Discussão do CVE escolhido na semana #2 CVE na aula TP

3 - Registo da caracterização anterior em LOGBOOK3.md no repo gitlab do grupo.

“””deve dar para identificação  
The vulnerability is due to insufficient sanitizing of user supplied inputs in the application when parsing HTTP requests. A remote attacker may be able to exploit this to execute arbitrary code within the context of the application, via a crafted request.  
“””  
  
“””  
A remote, unauthenticated attacker can execute operating system commands as root via crafted requests to the HTTP endpoint file\_transfer.cgi.  
“””

<hr>

1. Primeiro ponto
   1. Identification:
      1. OS Injection, a remote, unauthenticated attacker can use this vulnerability to execute operating system commands as root.
   2. Cataloguing:
      1. Autor: METASPLOIT
      2. Date: 30/04/2019
      3. How:
      4. Severity level: 9.8 according to NIST
   3. Exploit:
      1. https://www.exploit-db.com/exploits/46786
   4. Attacks:
      1. Successful attacks: The Crestron AM-100 firmware 1.6.0.2, Crestron AM-101 firmware 2.7.0.1, Barco wePresent WiPG-1000P firmware 2.3.0.10 etc.
      2. Documented example of an attack: <https://www.fortiguard.com/encyclopedia/ips/47830>

Used Links

https://threatpost.com/bugs-wireless-presentation-systems/144318/

https://vuldb.com/?id.134277

https://www.tenable.com/security/research/tra-2019-20

https://www.trendmicro.com/vinfo/hk/threat-encyclopedia/network/ddi-rule-2936

https://www.fortiguard.com/encyclopedia/ips/47830