NVD:美国漏洞数据库

漏洞列表：<https://nvd.nist.gov/vuln/full-listing>

查看漏洞信息：以CVE-2022-2274为例<https://nvd.nist.gov/vuln/detail/CVE-2022-2274>

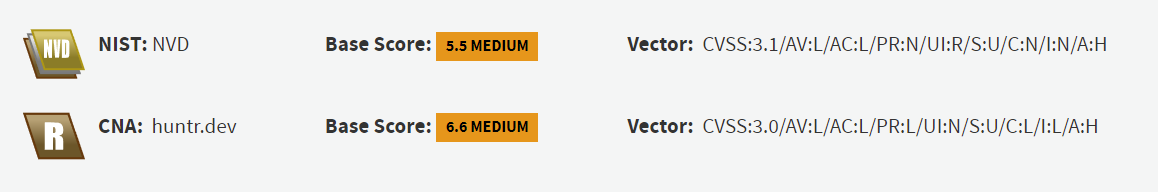
包含

* 漏洞描述：

The OpenSSL 3.0.4 release introduced a serious bug in the RSA implementation for X86\_64 CPUs supporting the AVX512IFMA instructions. This issue makes the RSA implementation with 2048 bit private keys incorrect on such machines and memory corruption will happen during the computation. As a consequence of the memory corruption an attacker may be able to trigger a remote code execution on the machine performing the computation. SSL/TLS servers or other servers using 2048 bit RSA private keys running on machines supporting AVX512IFMA instructions of the X86\_64 architecture are affected by this issue.

* 分析描述：（一般与漏洞描述相同）
* 漏洞严重性评估

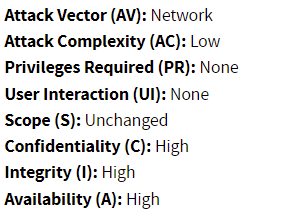
可能包含多个评估方？如NIST与CAN



* + CVSS 3.x
    - 得分： 9.8 critical



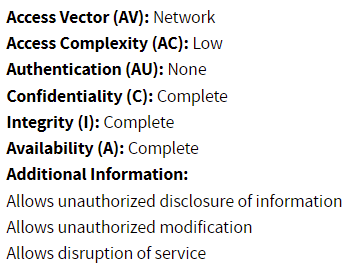
* + - Vector：



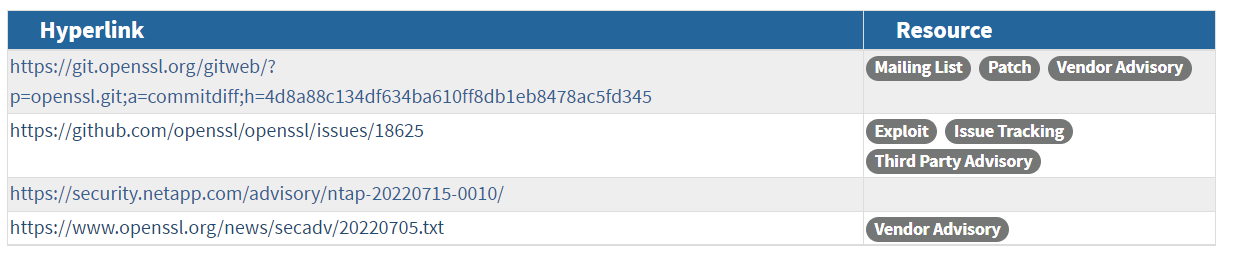
* + CVSS 2.0
    - 得分：10.0 High



* + - Vector：



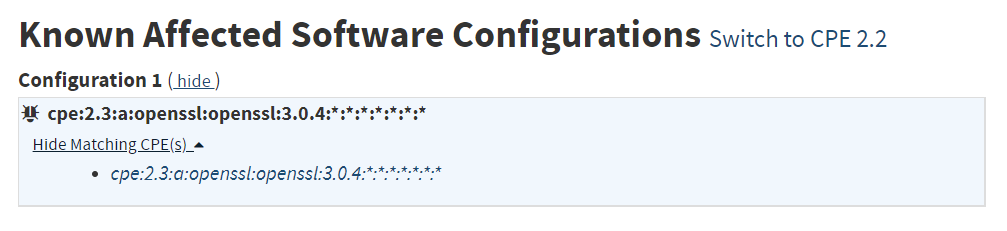
* 外部网站信息
  + Patch
  + Vendor advisory
  + Exploit



* 漏洞类型

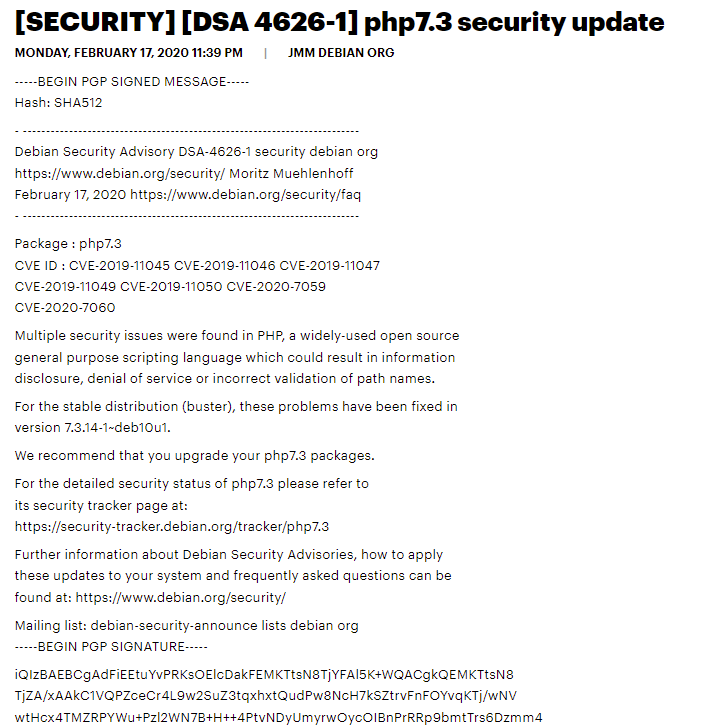


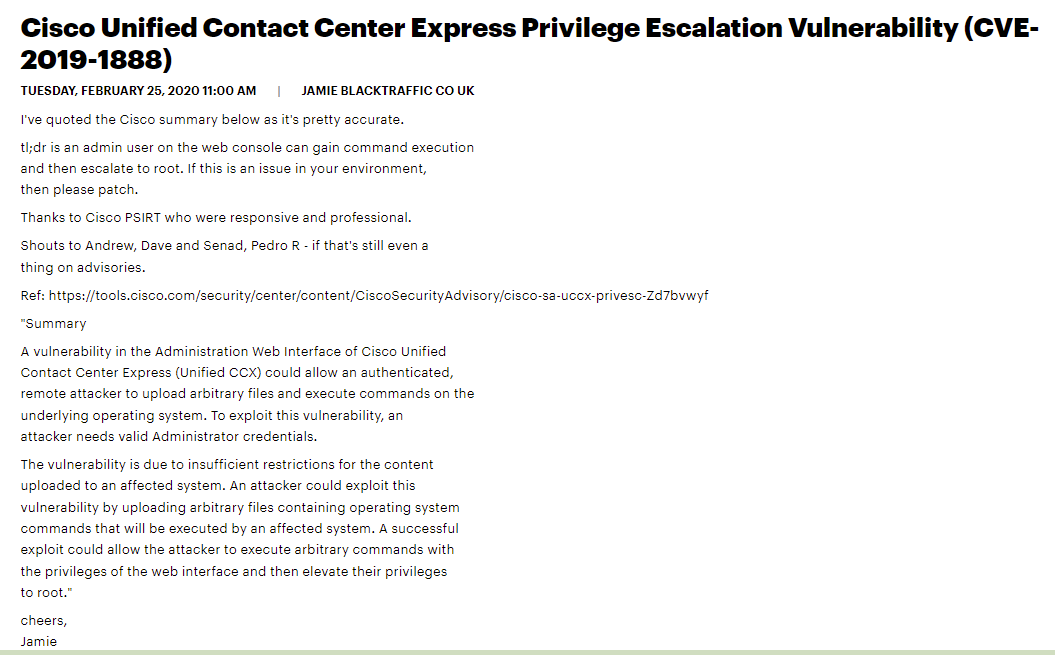
* 受影响的软件



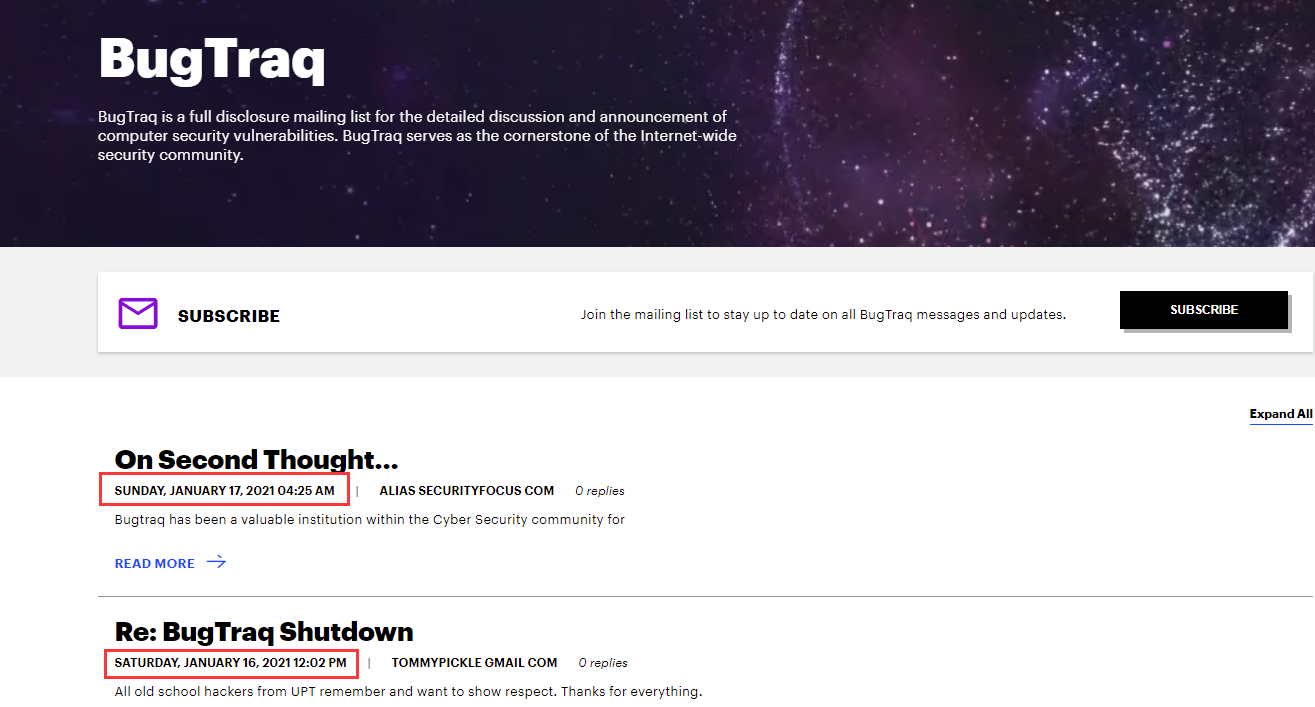
SecurityFocus：一个安全社区？ <https://bugtraq.securityfocus.com/archive>

一些对于漏洞的分享？





不过貌似近期没有更新

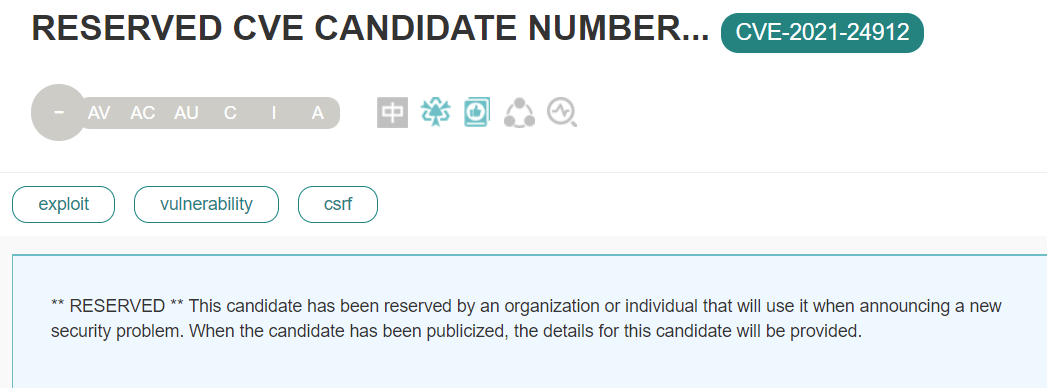


信息安全漏洞门户 vulhub

<http://vulhub.org.cn/index>

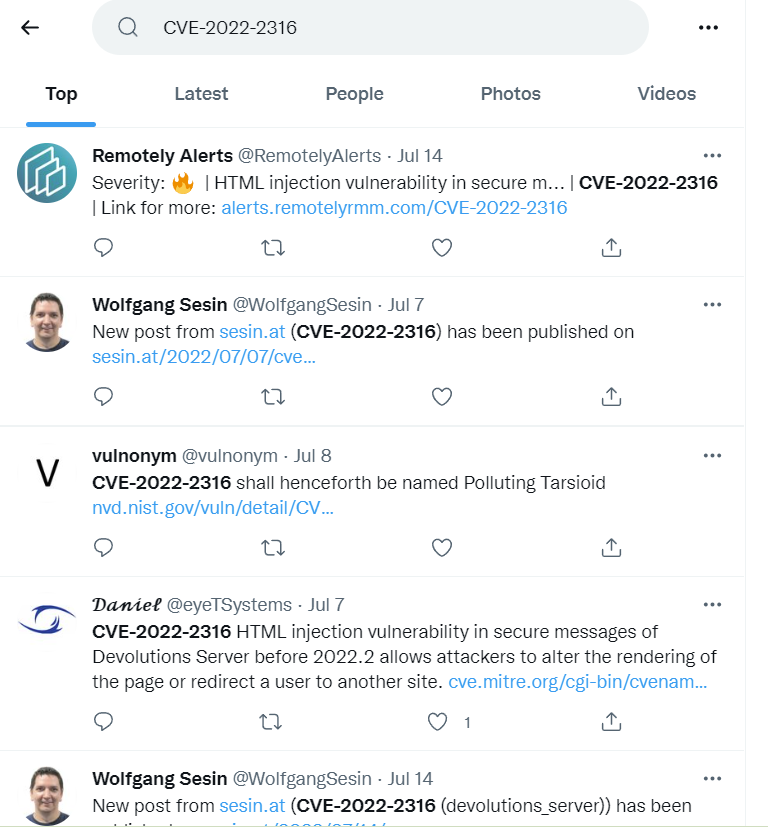
=========================





Twitter

用CVE号搜索推文



新浪微博



