**漏洞風險報告**

**IP : 140.138.144.66**

**Organization : Taiwan Academic Network**

**Operating System : None**

**Country :Taiwan**

|  |  |  |  |
| --- | --- | --- | --- |
| **CVE名稱** | **CVSS** | **討論程度** | **exploits** |
| **CVE-2010-1899** | **V2.0:**4.3 中  **V3.X:** N/A | **Twitter:13**  **Stackoverflow:1** | **No** |
| **CVE-2010-2730** | **V2.0:**9.3高  **V3.X:** N/A | **Twitter:11**  **Stackoverflow:0** | **No** |
| **CVE-2010-3972** | **V2.0:**10.0 高  **V3.X:** N/A | **Twitter:17**  **Stackoverflow:0** | **Yes** |
| **CVE-2012-2531** | **V2.0:**2.1 低  **V3.X:** N/A | **Twitter:14**  **Stackoverflow:0** | **No** |
| **CVE-2012-2532** | **V2.0:**5.0 中  **V3.X:** N/A | **Twitter:16**  **Stackoverflow:0** | **No** |
| **CVE-2010-1256** | **V2.0:**8.5 高  **V3.X:** N/A | **Twitter:11**  **Stackoverflow:0** | **No** |
| **CVE-2017-11882** | **V2.0:**9.3 高  **V3.X:**7.8 高 | **Twitter: 100+**  **Stackoverflow:0** | **Yes** |
| **CVE-2020-1350** | **V2.0:**10.0高  **V3.X:**10.0 高 | **Twitter:100+**  **Stackoverflow:1** | **No** |

1. **CVE-2017-11882:**

**描述:**

Heap-based buffer overflow in the TELNET\_STREAM\_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information.

**弱點枚舉:**

CWE-119

**exploits:**

<https://www.exploit-db.com/exploits/43163>

**最相關的Twitter文章:**

**發布者:**

Craig Williams

上午3:50 · 2020年2月13日

**內容:**

Talos has observed a malware campaign that utilizes a new version of Loda RAT exploiting CVE-2017-11882 deets here –

[https://blog.talosintelligence.com/2020/02/loda-rat-grows-up.html](https://blog.talosintelligence.com/2020/02/loda-rat-grows-up.html%20)

Nice job @g0jirasan

#LodaRAT

**Twitter共有100+篇文章。**

**最相關的Stackoverflow文章:**

NONE

**Stackoverflow共有0篇。**

1. **CVE-2020-1350:**

**描述:**

A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests, aka 'Windows DNS Server Remote Code Execution Vulnerability'.

**弱點枚舉:**

CWE-119

**exploits:**

None

**最相關的Twitter文章:**

**發布者:**

Worawit Wang

下午11:42 · 2020年9月25日

**內容:**

Exploit writeup of #SIGRed (CVE-2020-1350) #RCE on Windows 2012/2016/2019

<https://medium.com/@datafarm.cybersecurity/exploiting-sigred-cve-2020-1350-on-windows-server-2012-2016-2019-80dd88594228>

**Twitter共有100+篇文章。**

**最相關的Stackoverflow文章:**

**None**

NONE

**Stackoverflow共有0篇。**