RE: VMG5153-B30B 缓冲区溢出漏洞

3 封邮件

security <security@zyxel.com.tw> 2020年9月17日 下午6:20
收件人：杨超 <firmianay@gmail.com>
抄送：security <security@zyxel.com.tw>

Hi楊超,

再次感謝您的通報，經內部驗證後確認存在有緩衝區溢出問題，但在VMG5313-B30B的原廠設定中，HTTP 遠端連線預設為關閉， 況且產品本身有認證與隨機產生會話密鑰(session key) 的機制，因此風險較低。且VMG5313-B30B系列機種已EOL，根據產品EOL作業程序，我們將不再提供正式修補程式。謝謝!

Regards,

Zyxel Security Team

From: security
Sent: Thursday, September 03, 2020 10:59 AM
To: 杨超 <firmianay@gmail.com>
Cc: security <security@zyxel.com.tw>
Subject: RE: VMG5153-B30B 缓冲区溢出漏洞

Hi楊超,

感謝您的通報，我們會請相關團隊進行驗證，有任何進一步消息再與您聯繫，謝謝。

Regards,

Zyxel Security Team

From: 杨超 [mailto:firmianay@gmail.com]
Sent: Wednesday, September 02, 2020 4:51 PM
To: security <security@zyxel.com.tw>
Subject: VMG5153-B30B 缓冲区溢出漏洞

你好，我在 VMG5313-B30B_5.11(ABCU.1)C0 中发现一个疑似缓冲区溢出，位于 zhttpd 程序的 FUN_00405218，该函数用于导入本地CA证书，URI 构造应该类似 “/cgi-bin/Certificates?action=import_local&priv=xxxxxxxx”，由于程序采用 while 的方式寻找字符串 “xxxxxxxx”的结尾（&、?、\0），然后直接与字符串开头相减作为 strncpy 函数的长度参数，如果字符串过长，可能导致溢出。

遗憾的是我没有真实设备进行测试，但我非常相信这个漏洞的存在，所以先发了这封邮件。期待你们的回复。

杨超 <firmianay@gmail.com> 2020年9月17日 下午8:00
收件人：security <security@zyxel.com.tw>

感谢回复，其实我是看过这篇文章（https://blog.somegeneric.ninja/Zyxel_VMG5153_B30B）后才下载的固件，那么这个问题是否也可以分配一个CVE呢?

security <security@zyxel.com.tw> 于2020年9月17日周四 下午6:20写道：
[引用文字已隐藏]

---

security <security@zyxel.com.tw> 2020年9月18日 上午9:55
收件人：杨超 <firmianay@gmail.com>
抄送：security <security@zyxel.com.tw>

HI 楊超,

感謝您的回覆。關於CVE ID部分，因為漏洞是由您發現，建議由您申請會較為合適。若有任何問題，請再與我們聯絡，再次感謝您直接通報給Zyxel。

[引用文字已隐藏]