Raffica di vulnerabilità nei driver Asus e Gigabyte, ma niente patch…

Dic 20, 2018 Marco Schiaffino News, RSS, Vulnerabilità 0

I bug consentono di eseguire codice in remoto e aumentare i privilegi sul sistema. I due produttori, però, non stanno prendendo contromisure adeguate.

Alle orecchie degli esperti di sicurezza, le falle di sicurezza relative ai driver di componenti come motherboard e schede video fanno suonare un campanello di allarme particolarmente acuto.

Si tratta, infatti, di componenti software che gli utenti aggiornano con frequenza minore rispetto alle normali applicazioni e che rischiano di conservare le vulnerabilità per lunghi periodi.

A turbare i sonni degli addetti ai lavori, oggi, sono quattro driver di **Asus** e **Gigabyte**, che complessivamente collezionano la bellezza di sette vulnerabilità che i pirati informatici potrebbero sfruttare per portare vari tipi di attacchi.

Per quanto riguarda **Asus**, i problemi si annidano in **Aura Sync**, un software pensato per gli ultra-impallinati di modding e che consente di sincronizzare gli effetti di illuminazione di schede video, schede madri, mouse e tastiere.

Al momento dell'installazione, il software implementa due driver chiamati **GLCKIo** e **Asusgio**. È proprio in questi componenti che si annidano tre vulnerabilità (CVE-2018-18537, CVE-2018-18536, CVE-2018-18535) che consentono di avviare

l’esecuzione di codice sulla macchina.

I ricercatori di **SecurAuth** che hanno individuato le vulnerabilità hanno anche realizzato un Proof of Concept (PoC) che dimostra il funzionamento dell’exploit. **Il codice che hanno realizzato si limita a eseguire uno shutdown del sistema, ma la procedura consentirebbe di compiere anche azioni più dannose**.

La vulnerabilità più grave, però, è quella che affligge Asusgio (CVE-2018-18535). L’esecuzione di codice, infatti, in questo caso avviene con i massimi privilegi (ring-0), cioè **a livello di kernel**. Il PoC messo a punto dai ricercatori, in questo caso, **provoca un crash immediato del sistema**.

Le vulnerabilità sono presenti in Aura Sync fino alla v1.07.22 (quella attualmente indicata come la più aggiornata). La nuova versione (1.07.22.1) è infatti ancora in fase di Beta e contiene la patch solo per uno dei due driver vulnerabili.

Le cose non vanno molto meglio con **Gigabyte**, che secondo i ricercatori avrebbe addirittura negato il problema dopo le comunicazioni intercorse.

E non si tratta di un problema da poco. Tutte le falle riguardano l'interazione tra i driver (GPCIDrv e GDrv) e altri processi che girano sul sistema, anche quelli che Windows considera "non affidabili". I driver in questione sono utilizzati dal **GIGABYTE APP Center**, dal **XTREME GAMING ENGINE**, da **OC GURU II** e dall'**AORUS GRAPHICS ENGINE**.

Una delle vulnerabilità che affligge GDrv (CVE-2018-19320) permetterebbe addirittura di **prendere il completo controllo del sistema**, mentre la seconda (CVE-2018-19323) consente "solo" di elevare i privilegi di amministrazione nel sistema per **eseguire codice a livello kernel**.

Le ultime due vulnerabilità (CVE-2018-19321 e CVE-2018-19322) che affliggono entrambi i driver e hanno conseguenze simili alle precedenti due.

Anche in questo caso i ricercatori hanno pubblicato nel loro report anche il codice che dimostra il funzionamento degli exploit che hanno scoperto.

Please follow and like us:

Ondata di phishing prende di mira gli utenti Apple Attacco ai siti WordPress: i pirati inseriscono collegamenti nascosti

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2018/12/20/raffica-di-vulnerabilita-nei-driver-asus-e-gigabyte-e-per-alcune-non-ce-la-patch/