PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 616 di lunedì 09 settembre 2002

Falla nel sistema dei certificati digitali di Windows

Lo afferma un avviso di sicurezza di Microsoft. Gli amministratori di sistema devono installare la patch al piu' presto.

Sui sistemi di crittografia a chiave pubblica sono basate le tecniche attuali per la sicurezza delle comunicazioni sicure su Internet e funzionalità aggiuntive quali la firma elettronica.

Un Certificato Digitale è un file creato da un'entità indipendente, a cui viene riconosciuta fiducia da tutti gli enti interessati (Certificate Authority) ed il cui compito è garantire l'identità di colui che ne è in possesso.
Il certificato associa in modo protetto una chiave pubblica all'entità che possiede la chiave privata corrispondente. I certificati vengono firmati digitalmente dall'autorità di certificazione emittente e possono essere emessi per un utente, un computer o un servizio.
Il formato di questo file deve essere standardizzato e oggi lo standard più diffuso è quello stabilito dall'ente internazionale ITU-T e che è riconosciuto con la sigla X.509 versione 3.

In un bollettino di sicurezza diffuso il 4 settembre, Microsoft ha reso nota una seria vulnerabilita' individuata nel sistema dei certificati digitali di Windows.

Numerosi sono i software affetti dalla falla: Windows 98, Microsoft Windows 98 Second Edition, Microsoft Windows Me, Microsoft Windows NT 4.0, Microsoft Windows NT 4.0 - Terminal Server Edition, Microsoft Windows 2000, Microsoft Windows XP, Microsoft Office per Mac, Microsoft Internet Explorer per Mac, Microsoft Outlook Express per Mac.

La vulnerabilita', riguardante il controllo del campo "Basic Constrains" previsto dallo standard X.509, è definita critica in quanto consentirebbe ad un aggressore in possesso di un certificato digitale valido di creare un certificato con false informazioni riguardo alla propria identità.

Il certificato sarebbe accettato come valido dai sistemi nei quali la falla è presente; l'aggressore, ad esempio, potrebbe cosi' falsificare la firma digitale sulle e-mail o, nel caso di sistemi di autenticazione basato sui certificato, di elevare i propri privilegi.

Per eliminare la falla gli amministratori di sistema devono installare al piu' presto la patch messa a disposizione sul sito Microsoft relativa alla versione del software.

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.

---

www.puntosicuro.it