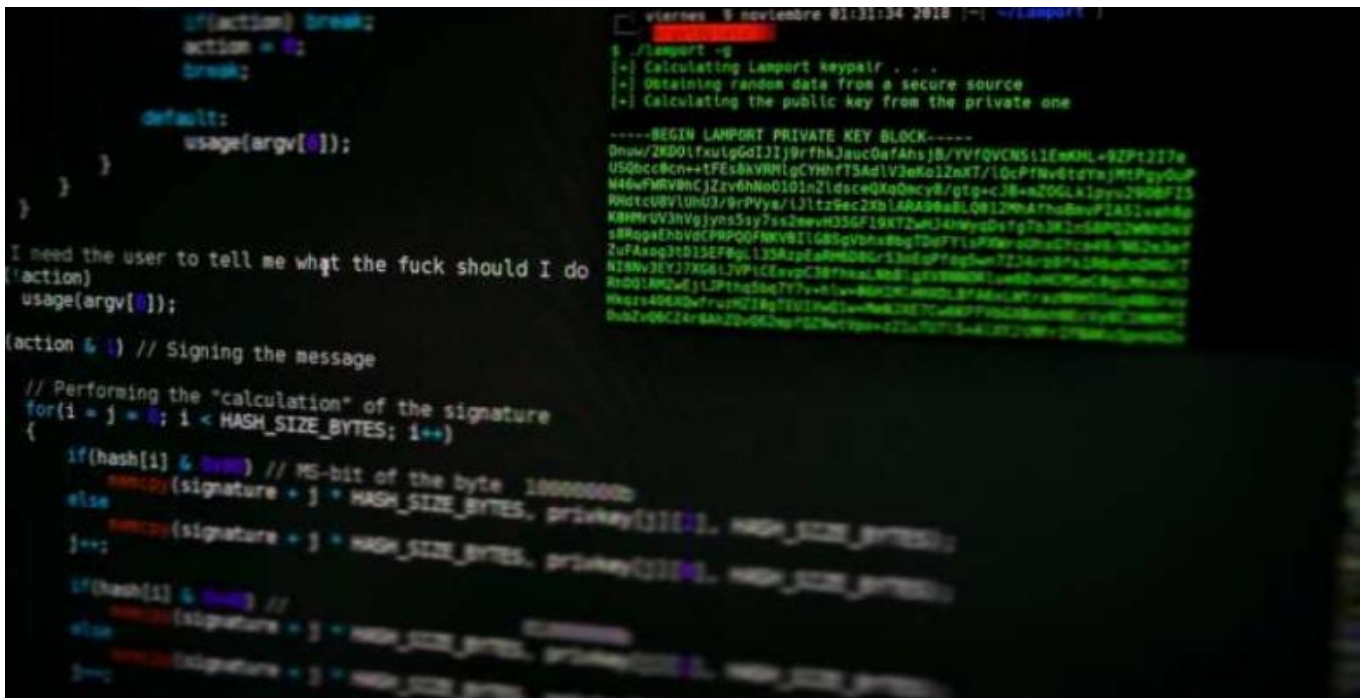


Brecha seguridad Windows descubierta por NSA

15/01/2020



```
if(action) break;
action = 0;
break;

default:
usage(argv[0]);
}
}

I need the user to tell me what the fuck should I do
action)
usage(argv[0]);

action & 1) // Signing the message
// Performing the "calculation" of the signature
for(i = j = 0; i < HASH_SIZE_BYTES; i++)
{
if(hash[i] & 0x01) // MS-bit of the byte 10000000
memcpy(signature + j + HASH_SIZE_BYTES, privatey[1][i], HASH_SIZE_BYTES);
else
memcpy(signature + j + HASH_SIZE_BYTES, privatey[0][i], HASH_SIZE_BYTES);
j++;
if(hash[i] & 0x02) //
else
}

vienes 9 noviembre 01:11:34 2018 j~| ~/Lamport /
$ ./Lamport -g
+ Calculating Lamport keypair . . .
+ Obtaining random data from a secure source
+ Calculating the public key from the private one

-----BEGIN LAMPORT PRIVATE KEY BLOCK-----
Dmaw/2K001fxu1gGdI3Ij9rfhk2auc0afAhsJB/YVfQVCNS11EwKML+9ZPt2I7e
US0cc8Cn++tFEs8kVRN1gCYhhFT5Ad1V2eK012xK7/10cPTNv6tdrjMtPgyDuP
N4dWfNRV8NcJZrv6hNo010In21dscQkQ0ncy8/rgtp+cJ8+n20GLk1pyu2906FIS
RhdTcUBV1UmU3/9rPyys/L3ltz9ec2XbLARAG9a8L09129hA7ha8vP1A511vnh8p
KBRm+V3Nvgjyns5iy7ss2eevH35GF19KT2wKJ4hWysDsfG7a3K1-5APQ2WwDky
sBRqpsEhbVcPRPQqFNvBI1G85GvBhs8bgTDeFTL1P8wv0ha07cwh-962a3ef
ZuFAxq3t013EF8q.135AxpEaR6D8Gr13adpPTAgDm7234rpd7a18q0c000-T
NIRv3EYJ7XG6L2VP1CExpC387haal8eB1gV9880L1u60vH00v0fPg_7h3u0D
RhdQ1AK2wEjL3Pthg5bg7Y7v+Vw+8kK0K7MMDL87AB6L87r+u0m03uq9880v
Hkzrs40E8Qw7ruH2T8gTE01h4G1+Ph6J8E7Cv88P7h0d08m861v0d1288m2
pubZv6C24r8aK2p+0K2hpT02hvt0p0+c22u70T15+4L3T208v1278a03p8h0K
```

Microsoft difundió una actualización de seguridad con la que repara una importante vulnerabilidad descubierta por la National Security Agency (NSA), agencia gubernamental de Estados Unidos que se ocupa de seguridad nacional.

La falla es en el sistema operativo Windows, que podría permitir que hackers violen o supervisen redes de computadoras.

Se trata del modo en que Microsoft usa las firmas digitales para verificar que el software sea auténtico.

Si se la aprovecha permite que los hackers falseen la firma ligada a partes del software, logrando hacer pasar un código malévolo como software legítimo.

Tanto Microsoft como la NSA dijeron no haber hallado pruebas de un uso malévolo, y exhortaron a instalar de inmediato los parches de seguridad para Windows 10, Windows Server 2016 y Windows Server 2019.