nominet

Key Roll issue

Roy Arends, Nominet UK

ff88313ad8>] :mca:mca_intr+0x447/0x457
ff80010b81>] handle_IRQ_event+0x51/0xa6
ff800b9d4d>] __do_IRQ+0xa4/0x103
ff8001235a>] __do_softirq+0x89/0x133
ff8006c9a3>] do_IRQ+0xe7/0xf5
ff8006b2d8>] default_idle+0x0/0x50
ff8005d615>] ret_from_intr+0x0/0xa
[<ffffffff8006b301>] default_idle+0x29/0x50
ff8004938f>] cpu_idle+0x95/0xb8
ff80076f7f>] start_secondary+0x498/0x4a7

September 10th 19:38:11

0e 48 89 e5 41 54 49 89 f4 53 48 89 fb 48 8d 7f 38
ffffff8008bb90>] dequeue_task+0x1/0x37
ff81002a53bf8>
0000000000000

kernel panic

This was related to an HSM driver

We were unable to reproduce the kernel panic

Hardware failures happen

That is why we over-provision

Critical, but no time pressure

Not a time-critical system

Two week signature expiry interval

Two simple failover scenarios:

Restart current signing system

Use active secondary signing system

Scenario 1: Restart the system

We have proper security hygiene

We require presence of a Security Officer

But... it was a friday evening

There was no time pressure

And there was an alternative scenario...

Scenario 2: Activate secondary system

Runs independent of main signing system

Pre-deployment checks

Everything was ready to go

But... it was a friday evening

And... there was still no time pressure

Saturday 11 september 2010

Decided to make the secondary system active

This would allow signing to continue

This gave us time to fix main signing system

No need for a Security Officer on-site

We started the signing system at 14:30

Something was not quite right

An unfortunate state

Main and secondary did not use same ZSK

Lead to some validation problems in the field

Quickly resolved by flushing the validator cache

Or wait until the key expires from the cache

This was unexpected and should not happen

Analysis

The Secondary system had a older ZSK

Signed properly by the KSK

It validates fine

The KEYSET had a 48 Hour TTL

Validators with keys from the main system could not validate signatures from the secondary system

Investigation

OpenDNSSEC consists of two parts:

Enforcer translates “policy” to configuration

Signer uses that config to sign the UK zone

Enforcer was unable to overwrite configuration

So the signer still uses the old ZSK

Investigation

Why has this not been flagged?

We use the auditor to check the zone status

We use ODS-HSMUTIL to list keys

We use ODS-KSMUTIL to report policy

No checks if a file could be overwritten

Additional Measures

Updated our audit scripts to include caching and monitoring to signal overwrite failures

TTL of the keyset down to 1 hour

No Sec. Officer to restart main signing system

Lessons learned

you can not test for everything beforehand

hardly anyone is validating DNSSEC yet

problems get very quickly fairly public

If you have this problem, have it on a weekend

This was not an OpenDNSSEC issue

Questions?

roy@nominet.org.uk