Tab 2 – Email trail

From: Unsworthy, Graeme <gunsworthy@spaldingsoftware.co.uk>
Date: 21 August 20:03
To: Kvitovich, Alex <akvitovich@spaldingsoftware.co.uk>; <madeline.l@ncsc.x.gis.gov.uk>
Cc: Smith, Jodie <jsmith3@spaldingsoftware.co.uk>
Subject: RE: Kobra bug

Alex,

Can we have a meeting tomorrow morning to discuss urgently? Jodie if you can attend and represent engineering that would be great.

Maddie – lovely seeing you at dinner last week. In the spirit of open communications between CNI-serving industries and the NCSC, I wanted to include you in this email chain. Please see Alex's email below for a summary and further emails for technical details. Would highly appreciate any advice you can provide in the matter.

All the best,

Graeme

Graeme Unsworthy

General Manager
Spalding Software Ltd.

From: Kvitovich, Alex <akvitovich@spaldingsoftware.co.uk>
Date: 20 August 17:56
To: Unsworthy, Graeme <gunsworthy@spaldingsoftware.co.uk>; Smith, Jodie <jsmith3@spaldingsoftware.co.uk>
Subject: FWD: Kobra bug
Priority: High

Graeme,

I need to loop you into this issue as we have a number of business-impacting decisions to make. Apologies for not consulting you until now, I have just got back from summer holiday (I can report Sicily is nice this time of year) and am working through a backlog of emails.

All details are contained in the email trail, but the gist of it is this:

- A software bug was reported to us from an external researcher
- The bug will allow an attacker to stop fuel flow at a facility
- Our team has confirmed the bug is in live production code affecting 55 customer facilities (37 UK, 18 international)
- We can fix the problem with a fast tracked patch, but it will take minimum 7 days to deploy

I need actions from you on the following:
1. Decide whether to fast track our patch or include it with regular periodic updates
2. Budget to schedule overtime for the engineering team if required
3. Decision on whether to acknowledge the researcher and whether to pay them
4. How we communicate this to customers
5. Whether we report to oversight and advisory bodies (don't you know someone at NCSC?)

Note that the researcher who discovered the bug has said they will publicly disclose it on 2 September unless they see evidence of action on our part, so time is now tight. We have no reason to believe this is an empty threat.

Thanks,

Alex

Alex Kvitovich

Chief Information Security Officer
Spalding Software Ltd.

From: Smith, Jodie <jsmith3@spaldingsoftware.co.uk>
Sent: 27 July 10:31
To: Kvitovich, Alex <akvitovich@spaldingsoftware.co.uk>
Cc: Chowdhury, Ishant <ichowdhury@spaldingsoftware.co.uk>
Subject: RE: Kobra bug
Priority: High

Hi Alex,

The engineering team has investigated the Kobra bug and rolled a patch into version 3.4.1. This is scheduled for deployment on 28th August, but I recommend forking our patches and postponing non-critical updates to 3.4.2 so we can deploy this update as soon as possible.

Note that version 3.3.8 and above are not affected, but uptake of this version is currently very low, only about 6% of total installed systems.

Let me know if you want to meet to discuss.

J

Jodie Smith

Engineering Manager
Spalding Software Ltd.

From: Chowdhury, Ishant <ichowdhury@spaldingsoftware.co.uk>
Date: 26 July 18:13

To: Smith, Jodie <jsmith3@spaldingsoftware.co.uk>
Subject: RE: Kobra bug
Priority: High

Jodie,

As mentioned this morning, we have investigated the Kobra bug report and engineered a fix. It is a critical issue so recommend patch deployment is fast tracked through the scrum process.

Jason omitted to say that the bug does not affect Kobra versions 3.3.8 and above.

Ish

Ishant Chowdhury

Senior Software Engineer
Spalding Software Ltd.

From: Mings, Jason <jmings@spaldingsoftware.co.uk>
Sent: 26 July 10:21
To: Chowdhury, Ishant <ichowdhury@spaldingsoftware.co.uk>
Subject: RE: Kobra bug

Hi Ishant,

I am putting this information into one email by way of tying up our conversations and the work we have done over the past couple of weeks.

This bug is now verified as accurate and live in deployed production code. Our data indicates 37 fuel distribution facilities in the UK are affected, with another 18 internationally.

We have conducted an investigation into how long it would take to patch all affected systems. Although executing the patch is relatively quick (less than 15 minutes), the patch requires that Spinnakers 10 to 19 are shut down and the system drained of fluid to reset measurement levels. This whole process can take anywhere between 4 to 8 hours depending on the size of the facility. This level of downtime is unacceptable on a systemic level (there would not be any fuel at hundreds of UK petrol stations), so the patch would have to be rolled out to one facility at a time. In other words, maximum 6 per day working around the clock, so a minimum of 7 days to get all facilities patched.

We have the patch ready to go in the form of Kobra version 3.4.1 and stand by to deploy as soon as we have approval.

Kind regards,

Jason

Jason Mings

Software Engineering Associate
Spalding Software Ltd.

From: Chowdhury, Ishant <ichowdhury@spaldingsoftware.co.uk>
Sent: 4 July 16:45
To: Mings, Jason <jmings@spaldingsoftware.co.uk>
Subject: RE: Kobra bug
Priority: High

Jason,

We have had a bug in Kobra reported to us via an external source. So far this is unverified but as you can see from the email trail management are hot on the case so we need to investigate pretty swiftly. You worked on the FlowCheck module right? Can you go into the source files and verify whether the reported bug matches production code?

I will schedule a meeting for tomorrow morning to scope out next steps.

Cheers,

Ish

Ishant Chowdhury

Senior Software Engineer
Spalding Software Ltd.

From: Smith, Jodie <jsmith3@spaldingsoftware.co.uk>
Sent: 4 July 12:10
To: Chowdhury, Ishant <ichowdhury@spaldingsoftware.co.uk>
Subject: FWD: Kobra bug
Priority: High

Hey Ish,

This has come in right from the top and looks pretty serious. Can you get your team on it ASAP to see the severity of the problem and how easy it would be to fix?

Thanks,

J

Jodie Smith

Engineering Manager
Spalding Software Ltd.

From: Kvitovich, Alex <akvitovich@spaldingsoftware.co.uk>
Sent: 4 July 09:15
To: Smith, Jodie <jsmith3@spaldingsoftware.co.uk>
Subject: FWD: Kobra bug
Priority: High

Jodie – please look into the below with high priority and report back to me.

Alex

Alex Kvitovich

Chief Information Security Officer
Spalding Software Ltd.

From: Contact <contact@spaldingsoftware.co.uk>
Sent: 1 July 08:59
To: Kvitovich, Alex <akvitovich@spaldingsoftware.co.uk>
Subject: FWD: Kobra bug

Dear Alex,

Please see the below which I think should be routed to you? Sorry it has taken so long to get to you, Jan has been on maternity leave so we haven't been monitoring the contact inbox.

Sam

Sam Wilderberry
Office Manager
Spalding Software Ltd.

From: 'robinsecthreats' <robinsecthreats@gmail.com>
Sent: 2 June 01:06
To: Contact <contact@spaldingsoftware.co.uk>
Subject: Kobra bug

To whom it may concern,

I'm an independent cyber security researcher specializing in ICS vulnerability detection and exploit mitigation techniques. For a couple of months now I've been looking at your Kobra DMS system. It was first shown to me at a hackathon but I don't know how the presenter got a copy of the source code in the first place. But that's not important, what is important is that I have discovered a critical bug in the software, details of which are below.

Module: FlowCheck

Class: getSpin16Val()
Code line: 571
Bug: `If Spin16 = OutVal.set then`
Suggested patch: `If Spin16 == OutVal.set then`
Confirmed in Kobra versions: 2.3.1, 2.4.2, 2.9.0, 3.0.2, 3.1.5

As you can see the code allows me to assign a value to Spinnaker16 rather than read the value. In simulated SCADA environments I have been able to use this vulnerability to disable fuel flow between primary pumps and outflow collection sources.

I disclose this to you in good faith that you will fix the problem as a priority. As far as I can tell you don't advertise a bug bounty, but it's good form to reward researchers who responsibly disclose bugs rather than sell them as vulnerabilities. I accept payment via PayPal. If I have not received a response from you within 3 months, or otherwise seen evidence that you have patched the bug, I will go public with the vulnerability. This is a generous amount of time.

Regards,

Robin Anderson – security researcher