Statement on Fujitsu remote support access to Post Office branch counters.

Dave Haywood, Security Architect

Post Office Account, Fujitsu

Date: 15-JUL-2015

Version: 0.4

Distribution:

Muhunda Satchithananda [Transition Office] (v0.1, v0.3)

Defence Legal [Chris Jay] (v0.1, v0.3)

Michael Harvey [Commercial Director] (v0.3)

Steve Parker [Strategic Support Lead] (v0.1, v0.3)

Pete Newsome [Managing Consultant] (v0.1, v0.3)

Andrew Thomas [Domain Architect]

Dave Spillett [Customer Solutions Architect] (v0.3)

History

Date	Version	Author	Description
13-JUL-2015	0.1	Dave Haywood	Initial draft issued for review
13-JUL-2015	0.2	Muhunda Satchithananda	Updates to v0.1 to Dave Haywood.
13-JUL-2015	0.3	Dave Haywood	Updates to v0.2. Issued for review.
15-JUL-2015	0.4	Dave Haywood	Updates to v0.3 based on feedback from MS, DL, PN, MH Informal review with Dave King @ Post Office

Accuracy

In the event that this document is shared outside of the Fujitsu account team it should be noted that whilst Fujitsu endeavours to ensure that the information contained in this document is accurate and correct, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

Scope

This paper describes the Fujitsu remote support access to Post Office branch counters under HNG-X and HNG-A.

HNG-X operation

Fujitsu have responsibility for the management and support of the branch counters under HNG-X.

The method used to access branch counters, for support purposes, is Secure Shell (SSH). SSH is a command line only utility that has no graphical component. The client component of the access resides on the support terminal servers (SSN) in the Ireland data centres. The server component resides on the branch counter and is provided by the Cygwin openSSH server package.

The Cygwin environment is used to support the branch counter application. SSH is used in response to an incident or as or as a proactive measure to investigate and resolve issues - for example, time synchronisation or disk errors, reported directly from branch counters via eventing.

Fujitsu are informed of potential issues via several routes:

- Systems Management Centre (SMC) calls
- Post Office calls raised call via ATOS
- Major Account Controller (MAC) team requests
- National Business Service Centre (NBSC) calls
- Events from counters

SSH is used by personnel from the Fujitsu Systems Support Centre (SSC) who have support tool access to aid in troubleshooting branch counter issues.

To gain access to the branch counter, using the remote support capability, the member of staff must:

- Be a Fujitsu employee
- Have been security and financially vetted
- Possess a 2 factor authentication token issued by the Security Operations team
- Have a valid Live environment Active Directory (AD) username and password
- Have access to an internal Fujitsu network (for Live support Terminal Server access)
- Have access to a branch support access private key
- Have knowledge of counter names / IP addresses

Cygwin is used to run diagnostic commands on the branch counter and read system and application logs. Typically, pre-constructed scripts are used to execute any commands on branch counters; this reduces the scope for human error and produces dependable output.

Cygwin is a modular product and only the components required for the remote support access are installed. Cygwin runs under a local user ID provisioned as part of the branch counter Gold Build. The local user id is a member of the local Windows Administrators group. Cygwin is therefore capable of running commands with the privilege of the local administrator. Postmasters do not have access to the Cygwin environment.

Cygwin has no access to the counter business application (CBA) graphical user interface (GUI) and Remote Desktop Protocol (RDP) is actively disabled as part of the branch counter Gold Build. The SSC support personnel have no knowledge of, or access to, the CBA passwords for users. The transactional logs for counters is stored within the data centres on the Audit Service, therefore no transactional data is held on the branch counter.

HNG-A operation

HNG-A is being developed to work within a multi-supplier Towers eco system. Under the EUC tower, the accountability for the provision of service and the accountability for management of the service is fragmented. The EUC operator has responsibility for the management and support of the Post Office branch infrastructure and the applications provider has the management responsibility for the CBA. In the transitional period the responsibility for managing the application remains with Fujitsu Services. The HNG-A application is part of the branch counter and as such, Fujitsu need remote support access to investigate any reported issues.

A number of changes are proposed to the remote support access to branch counters under the HNG-A gap analysis contractual terms (CT). These changes are driven by the change in support responsibility of the HNG-A counter and the removal of the IPsec VPN to branch counters. The changes (see DES/GEN/SPE/2745 - HNGA Counter Cygwin Specifications) include:

- Upgrading Cygwin to the latest version (this addresses known issues in OpenSSL and other products, protected in HNG-X by the IPsec VPN)
- Running the SSH server as a user who is not a member of the local administrators group
- Restricting SSH server access, through file system and registry permissions, to specific branch counter data sources (including log files) and directories
- Only allowing CBA specific services to be restarted
- Using a menu system on the SSN to perform specific branch counter support activities, rather than allowing users to directly invoke Cygwin commands
- Recording an incident number as part of the menu system activation
- Logging use of the menu system into the Windows event log
- Creation of a specific AD group to further restrict access to a branch support access private key

The reduction in capability is commensurate with the reduction in Fujitsu's responsibility for the management and support of the Post Office branch counters to just the CBA under HNG-A.

The Fujitsu SSC are still be able to read data pertaining to the HNG-X application but do not have access to other areas of the system, subject to access controls implemented by the EUC tower operator.

The additional auditing of remote support access may be used to report to Atos on the following support connection details:

- Incident reference number
- Date, time and duration of connection
- AD userid of user requesting the connection
- Target branch counter
- Menu activity selected