IP Office Technical Bulletin

Bulletin No: 161

Release Date: 24 December 2013

Region: Global

IP Office Security Vulnerability Notice

Avaya is aware of and is responding to a potential vulnerability of Avaya's IP Office, when Avaya's previously documented recommendations are not followed, in regards to recent SIP hacker attacks. These attacks have resulted in new extensions being created followed by unauthorized calls being placed.

IP Office supports an installation feature for automatic creation of extensions and user accounts. This feature is intended to be used during the initial system configuration and set-up only. It has come to our attention as a result of these recent events that some installed IP Office systems are not following Avaya's previously documented recommendation to disable this option when systems are placed into production service.

Immediate Recommendation
All systems deployed should be checked to ensure that the system has the feature for auto-create of extensions and users turned off. This is especially important if systems are reachable via the public Internet.

Ensure that auto create is disabled for both SIP and H.323 on all network Interfaces (LAN1 and LAN2). For LAN1 this feature can be found in the IPO Manager under the System/LAN1/VoIP tab. For LAN2 (the WAN port) the feature is found under the System/LAN2/VoIP tab.

Additional Recommendations

Implement a higher level of security protection:
Security is more than "hardening" the call platforms and should include a layering of defenses including the Avaya Session Border Controller for Enterprise (A SBCE) to create a SIP firewall.

Avaya further recommends that all IP Office owners and their support organizations check their system to ensure they meet the following Maximum Security settings in order to provide a higher level of protection.

Setup Maximum Security (recommended to provide the highest level of security)

Maximum Security settings ensure that IP Office servers and their associated Managers communicate only over connections protected by strong digital certificates with logging fully enabled. Furthermore, only certified individuals with

the correct service user name and password are permitted access to the servers from specific PC installations of IP Office Manager. These passwords cannot be simple.

To achieve a “Maximum Security” configuration, verify that each of the following activities and settings have been successfully completed:

- Change all default passwords of all service and security users. (See further explanation below)
- Set the system Security Administration service security level to Secure, High.
- Set the system Configuration service security level to Secure, High.
- Set the system service user Password Reject Action to Log and Disable Account.
- **Disable auto-create of SIP and H.323 extensions and user accounts**
- Set the system Client Certificate Checks level to High.
- Set the system Minimum Password Complexity to High.
- Set the system Minimum Password Length to >8.
- Set the system Previous Password Limit to non zero (>5).
- Set the system Password Change Period to non zero.
- Set the system Account Idle Time to non zero.
- Set the system Session ID Cache to zero.
- Set all User account passwords to be complex secure passwords that meet the “High Complexity” setting for minimum passwords.
- Install valid, 1024 bits (or 2048bit to meet new NIST 800-131A requirements), non self signed certificates derived from a trusted certification authority.
- Install the corresponding trusted CA certificate in each of the Manager’s windows certificate stores.
- Install the corresponding certificates in all the system Certificate Stores of all permissible Manager entities, and the trusted CA certificate.
- Disable LAN2 interface if not being used.
- Set Manager Certificate Checks level to high in Manager Security Preferences.
- Use IPO Security Manager to set the Certificate offered when installing a non self signed certificate.

  Refer to the IP Office Knowledge based for instruction on setting these options. The IP Office Knowledge Base can be found here.

Change Default Passwords

Changing default passwords is common practice, but often some accounts can be overlooked.

The following administrative accounts are defined on IP Office and Avaya recommends that the passwords for each of these accounts be changed with complex secure passwords before systems are placed into production service. Avaya recommends that the passwords similarly be changed for the administration accounts on B5800 Branch Gateway products (which are derived from IP Office)

Table 1. Service User accounts on IP Office

Account Details	Procedure Where to change
Username: security • Can the password be changed? Yes. • Warning if password is set to the default? Yes. • Required for Server Edition? Yes.	IPO Security Manager
Username: Administrator • Can the password be changed? Yes. • Warning if password is set to the default? Yes. • Required for Server Edition? Yes.	IPO Security Manager Web Manager
Username: Manager • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? No.	IPO Security Manager
Username: Operator • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? No.	• IPO Security Manager
Username: EnhTcpaService • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? Yes.	This account is required for Avaya one-X® Portal access to IP Office CTI. This account can be deleted or disabled if no Avaya one-X® Portal support is required.
Username: IPDECTService • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? Yes.	This account is required for DECT R4 access to IP Office configuration in provisioning mode. This account can be deleted or disabled if no DECT R4 support is required.

Username: SMGRB5800Admin • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? No.	This account is used for IP Office Branch Edition operation and for branching central manager (SMGR) access to web services. This account can be deleted or disabled.
Username: BusinessPartner • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? No.	IPO Security Manager.
Username: Maintainer • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? No.	IPO Security Manager
System Monitor **Username**: None. • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? Yes.	System monitor access The account cannot be deleted
VmPro **Username**: None. • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? Yes.	Vmpro configuration interface The account cannot be deleted, but access to the account can be disabled
Webcontrol **Username: Administrator** • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? Yes.	This account is used for IP Office Server Edition operation This account can be deleted or disabled.
Webcontrol **Username: root** • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? Yes.	This account is used for IP Office Server Edition operation This account can be deleted or disabled.

Branch (B5800) **Username: SMGRB5800Admin** • Can the password be changed? Yes. • Warning if password is set to the default? No. • Required for Server Edition? No.	This account is used in B5800 and in IP Office Branch deployments for Avaya Aura System Manager (SMGR) access to web services The account can be deleted or disabled

In addition to administration passwords, Avaya recommends that all User Account passcodes be changed to complex passcodes. If using numbers only, then the passcode should not contain consecutive or repeating numbers, numbers with easy to determine patterns, or numbers associated with the user's extension. Additionally, a numeric passcode should be at least 6-8 digits in length.

Examples of passcode to **not** use:

1234	Consecutive
123456	Consecutive
2580	TUI Pattern
159	TUI Pattern
0000	repeating
1435 if the extension is 1435 or 5341.	

Additional recommended steps

1. If SIP endpoints are not being used then unchecking the "SIP Registrar Enable" option can increase security. This should be done for interfaces that have Internet access. Note, that disabling this on both Interfaces (LAN1 and LAN2) will disable any SIP endpoint from registering with the IP Office.
2. Enable and use "User Rights" to control calling privileges. The Administrator can define limited calling as default rights of endpoints thus limiting calling to extension-to-extension and emergency only for example.
3. Ensure that the IP Office is not connected to the Internet without substantial data security deployed. A Session Border Controller to limit SIP exploits is also recommended as stated above.
4. Ensure TCP/UDP ports are well managed at the Internet firewall and follow the guidelines for TCP/UDP port usage documented in the IP Office Knowledge Base.

Security Improvements for newly deployed systems

Avaya has made changes to our 4Q13 service packs to disable "Auto-Create Extn/User" on IP500v2 systems by default. This may help to prevent further exploits on newly provisioned systems where previously documented recommendations have not been followed. Please note, however, that this will take effect only on new systems deployed with these service packs. If existing systems are upgraded to these service packs, the setting will **not** change as a result of the upgrade. Avaya therefore recommends that the settings described above always be checked and corrected if required after any system deployment or upgrade.

Issued by:
Avaya SME Customer Product Engineering Support
Contact details:-

EMEA/APAC

Email: ***gsstier4@avaya.com***

NA/CALA

Email: ***IPONACALAT4@avaya.com***

Internet: ***http://www.avaya.com***