General Management Interface

System Security Guide

http://www.gmi-foundation.org

GMI System Security Guide

This application note provides general information on the various security aspects and issues associated with the GMI Agent for general usage on a typical business network.

The GMI Agent program is intended as a general-purpose program that furnishes arbitrary access to end point data, and permits control over arbitrary portions of a managed platform. Accompanying significant power this is the need for special attention to security issues, necessary to prevent unauthorized access to data, as discussed herein.

Note! The GMI Agent, in the hands of a malicious user, especially when operating in a degraded security environment, can be dangerous! Misconfiguration of the GMI-Agent can compromise the security of a managed platform. It is of high importance to read and understand the information presented here.

These notes provide a general operating guide on how to securely implement the GMI Agent program.

Defense Against Unauthorized Use Of The Agent

After installing the GMI Agent program in any production environment, the operator should set the GMI Agent "/system/SecurityMode" value to 1, 2, or 3 to restrict access to the agent.

The GMI Agent "security modes" are explained in a variety of places (such as in the GMI-Agent DD) and briefly repeated here: A value of 0 (the default) provides no authentication; a value of 1 enables "password" authentication; a value of 2 enables the "IP allow list" authentication; a value of 3 enables both "passwords" and "IP allow list" authentication.

By default, the security mode of the agent is set to its lowest level = 0. The administrator should set the security mode of the agent to a higher level as a matter of routine. Failure to set a security mode will permit unauthorized access to the agent program, allowing any user to compromise the platform.

Note that many Apps will require a security mode greater than zero to operate. For example the "rshell.gmi", "psexec.gmi", and "msiexec.gmi" Apps, or any App installed in the "/control" path of the agent cannot be accessed unless the security mode has been

(at least) set to a non-zero value This safeguards against allowing access to more powerful Apps by unauthorized users.

Setting the Agent Password

One of the easiest ways to prevent unauthorized access to the agent is to set a security mode of 1 (or 3) for the agent, to enable password authentication. This causes the agent to check an accompanying password provided by each request to the agent.

Issue the following command at the GMI-Cmd.exe prompt:

```
GMI> set /security/securitymode = 1
```

After setting the security mode, the administrator should set a secret administrative password as follows:

```
GMI> set /security/passkey = (adminpassword)
```

After issuing the above command, the GMI-Cmd.exe program will disconnect the user. The user must reconnect with the correct password. (The GMI-Cmd.exe program will prompt for a password next time the user connects to the agent.)

The administrator can also set a "read-only" password, which permits programs to read from the agent, but not modify the agent configuration. The following command can be issued at a GMI command prompt:

```
GMI> set /system/passkeyreadonly = (userpassword)
```

Passwords can contain any characters and be up to 1000 characters in length. Leading and trailing spaces are stripped from the password. Caution should be taken when setting a password, because the password is not recoverable should it be forgotten by the user. In this case, the user may need to re-install the agent program, losing the static data associated with the agent.

Configuring the Agent IP Allow List

An alternative (or supplemental way) of restricting access, you may limit access to an agent to a small list of client addresses. This leverages the fact that within an enterprise, GMI Agents are normally used by only one or just a few command programs. To enable this mode of operation set a security mode of 2 (or 3) for the agent. Issue the following command at the GMI-Cmd.exe prompt:

```
GMI> set /security/securitymode = 2
```

After setting the security mode, the administrator can then upload a file containing a list of IP addresses (one IP address per line) to the "/security/IPAllowList" value.

```
GMI> upload /security/ipallowlist = (addresslistfile)
```

You can check the list of IP addresses that are allowed using the "ls" command:

```
GMI> ls /security/ipallowlist
```

The (addresslist) value is just a text file in standard "hosts" format, where an IP address is provided as the first value of each line, optionally followed by whitespace or a newline. Any entry in the file that is not an IP address is not entered into the list. The client address of the program that uploads the list is always included as an allowed IP address.

Note that, as an alternative to uploading an address list, the user can simply set the security mode back to 1 or zero, and then connect to the agent from each platform that will normally access the agent. This builds the list of allowed IP addresses. When the SecurityMode is set back to "2" or "3", no further updates occur and only those command programs that previously connected will be permitted access.

Configuring a Syslog Audit Trail

GMI contains a syslog interface that logs all connections, package installations and removals, as well as significant errors such as attempts to deny service, or invalid attempts to access the agent. The syslog interface sends standard syslog data to an SIEM or syslog receiver, furnishing a valuable audit trail of all activities on the system.

You configure the Syslog IP address (i.e. the location where to send syslog messages to) as follows:

```
GMI> set /security/sysloghosts = (ipaddr)
```

If you would like to have multiple syslog receivers configured for the program, you may upload a list of IP addresses (in standard "Hosts" format, as described previously) using the following command:

```
GMI> upload /security/sysloghosts = (addresslistfile)
```

Each syslog message contains (as part of the message content) the IP address of the client that accessed the agent, standard time of day, and the actual event that occurred. Severities of these syslog messages are selected appropriately, to indicate the nature of the message. The program uses the "system" facility for system type messages, and the "security" facility for access attempts.

Although a syslog audit trail is not strictly required by the GMI Agent, the functionality provided by configuring this function is extremely useful for general security management of the program.

Defenses Against Secret Installation of the GMI Agent

Implementation of security for is always a multi-layer approach; the security of a managed platform depends on various different factors ranging from good management of passwords, to careful deployment and maintenance of firewalls, as well as strong security awareness and logging.

For a bad actor to compromise a platform with a secret installation of the GMI Agent, there must exist multiple failures of an organization's security strategy. Specifically, a malicious must have permissions to modify firewall (to allow access to the standard GMI Agent port of 6441) and must have the ability to install a background service on a managed platform.

If both of these conditions exist, a bad actor can install GMI Agent and use it as a sophisticated "root kit" to conduct any number of dangerous activities. (Of course, if these conditions exist, other bad side effects are possible, such as installation of key loggers, network sniffers, or other dangerous software.)

The first line of defense against secret installation of the GMI Agent is to implement normal security practices, such as restricting non-privileged access, and maintaining a personal firewall on the managed platform.

In the extreme case where the malicious user has full access rights to the platform (for example a malicious system administrator exists in the organization), several defenses against secret installation of the program are built-in to the software.

- **Fixed Port Number.** The GMI Agent uses TCP port 6441 to listen for requests. End users cannot change this port number. This assists security officers in detecting installations of the program on a platform by simply looking for this port number via a port scanner or the "netstat –a" command.

- **Fixed Process Name.** The GMI Agent process name is fixed at "GMI-Agent.exe". The program will not operate under any other process name. Therefore, an administrator can simply check the process list (such as via the Windows "Task Manager") and look for this process. Attempts to rename the process will result in a failure to launch the agent.

- **Fixed Service Name**. The GMI Agent service name, in the Windows Service Manager, is fixed at "GMI Agent". Attempts to rename the service to some other value, or execute the agent under a different service name, will disable the operation of the agent. Therefore, an administrator can simply check the Windows Service Manager to detect whether this service name exists and has been enabled.

The above characteristics help prevent GMI Agent from executing on a platform under a hidden process name and / or service name, and prevent the GMI Agent from running

at a non-obvious port number. This assists with easily detecting whether the agent has been installed via simple inspection.

Conclusion

At GMI Foundation, we have carefully considered the security ramifications of releasing this software to the general public. We do not want to be in the business of creating software that supports hackers and criminals.

However, given today's security landscape, where personal firewalls are a standard part of modern operating systems, and advances such as "User Access Control" prevent non-privileged users from launching administrative programs, we feel that the GMI Agent program poses no substantial risk to any enterprise that has even naïve security awareness.

Additionally, the program attempts to promote good security by offering several compatible authentication options, and incorporating a logging interface that SIEM and security professionals will find extremely useful.

As with any software, latent security issues may exist. To facilitate easy upgrade, GMI embraces a "continuous improvement" philosophy with updates that correct for security (and other) deficiencies without sacrificing backward compatibility.

Parties interested in commenting on this document, or discussing security considerations related therein, are encouraged to contact GMI Foundation at the address below:

GMI Foundation
http://www.gmi-foundation.org
mailto: info@gmi-foundation.org