Bulletin No.: 2012-10-24 **October 24, 2012**

Unwanted Internet Request – Update

It is strongly recommended that any OfficeServ system that is configured to have a connection to the internet **must** be installed and properly protected behind a Firewall.

Our experience in Technical Support this week tells us that Internet requests from unwanted sources continue. A related bulletin was issued on Thursday of last week (10/11/2012) amidst reports of malicious attacks that did cause havoc and critical compromise to many business institutions within the United States. News sources today, continue to issue updates that those attacks are still happening. What we know about the attacks is that they are emanating from different sources globally. The malicious nature of the attack is that, the perpetrating application first "Sniffs" out vulnerable IP Addresses and then later follows up by bombarding those specific addressed with thousands of requests via SNMP protocol. Any processor on the internet that is exposed to these messages and designed to respond will essentially be "Choked" because of the sheer volume of these requests and not be able to perform any other of its necessary duties.

The resolution therefore is to isolate any system from being affected. Our bulletin of 10/11/2012 informed you to do just that:

If you have customers that have been affected by this trouble, you can address it using the following options:

- Disconnect the system from the Internet
- Re-assign the Public IP address (This might be a temporary solution as the new address may become a future target)
- Set firewall settings to isolate the OfficeServ system from SNPM traffic (ports 161 and 162)

Unwanted Internet Request - Update

The results:

- Disconnecting systems from the internet has been 100% effective.
- Reassigning the Public IP address has been effective but, as warned, has left the system vulnerable to future attacks which, in some cases, we have indeed now observed.
- Ports 161 and 162 are ports that are formally assigned to SNMP traffic. Using a firewall to block ports 161/2 is effective for this particular violation experienced in this spate of attacks. It should be pointed out though, that a future attack might be designed to adopt another form messaging and so addressing just these ports is not the most secure solution.

A more secure method to provide security was the subject of the bulletin released on 10/16/2012. It essentially detailed all the port numbers that are used by the OfficeServ product and advised the use of a dedicated firewall. In this application the firewall is programmed to only allow access by ports used on the OfficeServ. Care should be taken over the firewall element in this implementation. If a firewall/router is used, consideration must be given to the overall LAN design and applications in use. It is because if a router is employed "WAN" and "LAN" sides of the router will have different addresses and may cause complications in a SIP environment for example. Therefore with a dedicated firewall for the OfficeServ using a transparent or layer 2 firewall (no router) is a simpler approach.

Using the Customer's Firewall

In most cases, where the OfficeServ is positioned behind the customer's firewall, effective security can be applied directly to the customer's firewall. The customer's IT department can, be requested to configure it so that for the IP traffic associated with the OfficeServ's IP address, only the ports assigned to the OfficeServ will be allowed. (Please see on the next page) This is likely the most cost effective way for you to address the issue as it will most likely not require a site visit.

NOW AVAILABLE ON VIDEO!

Please login to **GSBN** (samsunggsbn.com), navigate to **Communication**>>**Training**>> **Videos**>>**Archived**>>**Setting Up a Firewall for OfficeServ**, to view a video of setting up a typical firewall for protecting an OfficeServ system in a data network. It is there as an aid as you will need to adopt similar consideration to any firewall you may set up in to provide security OfficeServ.

For support configuring your specific router/firewall contact the router/firewall manufacturer.

Unwanted Internet Request - Update

Please be aware that Samsung cannot be responsible for unwanted Internet requests or for the integration of OfficeServ in a networked environment. You should consider the security of your installed systems to be a high priority. Make sure any system connected to the Internet is properly protected behind a firewall.

Refer to the System Port Usage table below.

SYSTEM PORT USAGE

Module	Service	Protocol	Port
MP	SIP	UDP/TCP TCP	5060 5061
	H.323	TCP UDP	1720 1719
	SPNET	TCP	6100
	ITP	UDP	6000, 9000
	WIP	UDP	8000, 8001
	MVS	TCP	9012
	DM	TCP	5090,5091
	DM FTP	TCP	21
	DM Data	TCP	5090
	DM File Control	TCP	5003
	DM Embedded VM	TCP	6001, 6002
	ITT	TCP	5090, 5091
MGI16 MGI64 OAS	MGI	UDP	30000~ (2*Num of Ch -1)
	MPS	UDP	40000~ (2*Num ofCh -1)
	RTG	UDP	45000 ~ (2*Num of Ch-1)
CNF24	Conference	UDP	30000 ~ (2*Num of Ch -1)
	FTP	TCP	21
	Upgrade Port	TCP	60000
SVMi-20i	VM Control	TCP	6001,6002
	VM	UDP	30000 ~ (2*Num of Ch -1)
	FTP	TCP	21
	Upgrade port	TCP	60024

Samsung Telecommunications America
Business Communications Systems
1301 East Lookout Drive
Richardson, TX 75082