



SANS is the most trusted & by far the largest source for information security, audit, training, certification & research in the world.

Note: Hundreds of millions of devices are being placed on networks with built-in back doors. Printers, routers, computers, control systems, storage systems, medical devices, nearly every automated device has them. The manufacturers of these systems never told you how vulnerable you are. One victim said "It's as if the people who are supposed to help me put a big sign on my door saying 'the key is under the mat by the back door,' and anyone can come in and violate me and my family." These vulnerable back doors were installed to allow remote management; they are fully functioning processors with network connections, operating systems, and memory. In addition to being able to disable the device, in many cases they provide remote back-door access to the main CPU and storage of the computer or other device. A research program is being launched to find and close the secret back doors. This is one of the most critical technical research projects we've announced in NewsBites - and SANS has allocated \$20,000 in immediate grants for people (anywhere in the world) who can help develop answers quickly. If you think you have data or skills that can help, please read the last story in this issue.

Alan

Closing the Back Doors in Printers, Computers, and Appliances

Hundreds of millions of devices are being placed on networks with built-in back doors. Printers, routers, computers, control systems, storage systems, medical devices, nearly every automated device has them. The manufacturers of these systems never told you how vulnerable you are. One victim said "It's as if the people who are supposed to help me put a big sign on my door saying 'the key is under the mat by the back door,' and anyone can come in and violate me and my family." These vulnerable back doors were installed to allow remote management; they are fully functioning processors with network connections, operating systems, and memory. In addition to being able to disable the device, in many cases they provide remote back-door access to the main CPU and storage of the computer or other device. They may not be logged or monitored and therefore can be attacked repeatedly without fear of being caught. In Intel-based PCs and servers they are usually called BMCs, or baseboard management controllers and are used as intelligent controllers for inventory, monitoring, logging, and recovery control functions available independent of the main processors, BIOS, and operating system. Similar functions are provided on UNIX systems, and on printers and medical devices and other appliances but are often not called BMCs. This research project is designed to develop detailed technical procurement language that organizations can use to ensure these back doors are "closed and locked" when the devices are delivered. These back doors have already been implicated as attackers in successful denial of service tools and can be used to access and change the data being processed by the devices.

Here are initial research questions that need to be answered. If you think of other important questions, please propose them.

1. What are the vulnerabilities of these back doors (Telnet, FTP, hard coded passwords, etc.) and how can they be exploited. This should be done within device family - for smart printers for example
2. What types of damage can be done by an attacker who gains a foothold through these back doors.
3. How could an attacker jump from the back door processor to the main processor, or extract or change data being processed by the main processor or storage systems of the computer or appliance?
4. What are the most important security controls that must be engineered into every such device to protect them from remote or local exploitation?

If you have run tests on these back doors or have the access, tools and willingness to do so quickly, email apaller@sans.org We can provide funding for the work.