IOActive Security Advisory

Title	SIEMENS Sipass Integrated 2.6 Ethernet Bus Arbitrary Pointer Dereference
Severity	Critical
Discovered by	Lucas Apa
Date Reported	09/11/12
CVE	TBD
Siemens Advisory	SSA-938777

Introduction

SIEMENS SiPass® Integrated is an extremely powerful and flexible access control system that provides a very high level of security without compromising convenience and ease of access for system users. As a result, thousands of corporations, airports, ports, government agencies, hospitals, universities, and other organizations worldwide are using SiPass integrated access control systems. The system also provides a complete range of reports and can handle a large number of external controls, including elevator controls, alarm outputs, machine controls, and fire alarm inputs.

Affected Products

SIEMENS SiPass Integrated MP2.6 and earlier

Threat and Impact

The vulnerability exists within AscoServer.exe during the handling of RPC messages over the Ethernet Bus. Insufficient sanity checking allows remote and unauthenticated attackers to corrupt a Heap-Allocated Structure and then dereference an arbitrary pointer.

This flaw allows remote attackers to execute arbitrary code on the target system, under the context of the SYSTEM account, where the vulnerable versions of SIEMENS SiPass Integrated are installed.

More advanced payloads could modify the behavior of the application's internal controllers to unlock doors, control specific hardware, or expose businesses to other security risks.

Technical Details

The main communication channel that the Server uses to communicate with ACC Controllers is Ethernet. Each controller sends and receives messages to and from the Server and the hardware devices that monitor the system. All the components used in the SiPass integrated system are ultimately connected to the Server.

There is virtually no limit to the total number of controllers that can be connected. Various networking options (LAN/WAN/PSTN) can expand the system to include buildings and locations all over the world.

AscoServer is the executable used by the SiPass server that acts as the gateway to remotely access SiPass resources on port 4343.

The Ethernet Bus library connects the Server to the advanced Central Controllers (ACC) and allows communication between the Server and defined devices and points. Ethernet communication means that AscoServer doesn't need a dedicated Bus, because both Windows and the ACC understand the TCP/IP protocol used to send and receive messages over Ethernet networks.

After creating an I/O completion port with an existing file descriptor, the server begins listening for IOCP messages on that port. When the server receives an IOCP message, it creates substructure elements that are copied into shared memory between threads.

Due to insufficient sanity checking when manipulating an IOCP message, it is possible to alter the behavior of message parsing, allowing another IOCP message to subvert the listener of IOCP messages, leading to export of a write-n primitive.

```
0BD0F8B4   0B44A7A1  /CALL to memcpy from Ethernet.0B44A79C
0BD0F8B8   0000FE00  |dest = [[[[[user controlled ptr]]]]
0BD0F8BC   0BF0D5D0  |src = 0BF0D5D0 # [[[[[ptr to content]]]]]
0BD0F8C0   00000BB8  \n = BB8 (3000.)
```

This allows an attacker to write arbitrary data within the application, leading to remote code execution. Since the application spawns multiple threads for handling Ethernet connections, one approach for exploiting the vulnerability would be to overwrite a pointer to the first exception handler in any of the Thread Environment Block (TEB) structures and seize control of the exception-handling thread after an access violation. Even though Thread data blocks are randomized, addresses are stable because multiple identical threads are created.

Remediation

For customers of SiPass integrated MP2.4, MP2.5 and MP2.6, Siemens provides a software hotfix that fixes the vulnerability. Please contact customer support to acquire this hotfix. Siemens recommends that customers with earlier versions of SiPass integrated upgrade to one of the above versions. To acquire the software hotfix for SiPass integrated, please contact customer support at:

- sp.support.de@siemens.com