

RSUPPORT RemoteCall

# Security white paper

## RSUPPORT의 신제품으로 더 쉽게 다가가십시오.

원격지원의 선두주자 알서포트가 원격지원 시장의 새로운 니즈에 부합하는 다양한 2009년 신제품 라인을 제공합니다.

**RemoteHelp** - 인터넷을 통한 가상 헬프데스크입니다. 일반 상담원과 전문 상담원을 구분 배치하여 효율을 높일 수 있는 대형 콜센터 용 상담지원도구로 상담 대기 및 자동 분배가 포함된 고급 원격지원 도구입니다

**RemoteCall 5.0** - 일반 사용자부터 전문가까지 누구나 쉽게 웹 브라우저를 통해 상담원과 고객의 컴퓨터를 연결하여 지원할 수 있는 원격 커뮤니케이션 도구입니다.

**RemoteSales** - 온라인 상으로 고객과 마주하여 세일즈가 가능하게 해주는 신개념의 세일즈 도구로 언제 어디서나 쉽게 원격으로 프리젠테이션을 가능하여 고객과의 커뮤니케이션에 있어 최단시간에 최대효과를 꾀할 수 있는 도구입니다.

<http://www.rsupport.com>

좀더 자세한 정보는 RSUPPORT의 홈페이지에서 확인할 수 있습니다.

## Go Secure with RSUPPORT

### 배경

일반 사용자부터 전문가까지 누구나 쉽게 웹 브라우저를 통해 상담원과 고객의 컴퓨터를 연결하여 지원할 수 있는 원격 커뮤니케이션 도구입니다.

알서포트의 제품군은 웹서비스가 가지는 아래에서 설명되는 다양한 보안상 취약점에 대해 완벽히 차단한 원격지원 서비스를 제공합니다.

### ActiveX 취약점이란?

ActiveX는 1996년 초에 발표되었으며, 잘 알려진 바와 같이 ActiveX는 COM (Component Object Model)의 확장판의 성격을 가지며, DCOM (Distributed COM)을 거쳐서 현재의 .NET 전략으로 통합되는 양상을 띄고 있습니다. 사실상 ActiveX는 SUN의 JAVA에 대한 대안의 성격으로 발표된 것으로 보입니다. 당시 마이크로소프트의 API 혁명이라고 불릴만한 OLE (Object Linking and Embedding) 기술은 OLE로 연결된 개체가 다른 응용프로그램에서도 적용되고, 작동될 수 있도록 하는 것을 의미합니다.

ActiveX는 신뢰모델에 기반합니다. MS는 서명된 ActiveX 컨트롤은 허용하고, 서명되지 않은 ActiveX는 불허하는 방식을 취합니다. 서명된 ActiveX가 악의적인 코드가 포함되어 있지 않다는 조건을 만족했을 때 가능한 모델입니다.

기존에 발견된 ActiveX 컨트롤 취약점은 아래와 같습니다.

1. 로컬 자원에 접근 가능한 Method 를 직접적으로 제공
2. 업데이트 기능을 악용하여, 정상적인 배포본이 아닌 조작된 배포본을 받게 하는 행위
3. 정교하게 조작된 입력값을 통해 정상적 로직을 Bypass 하는 경우
4. Method나 Property 등의 입력 값에 대한 버퍼 오버플로우의 취약점을 이용하는 경우
5. MS 사이트의 취약점을 통해 설치가 가능한 악성코드 배포 (Black ActiveX)를 삽입하고, 사이트 방문자 모두에게 취약성에 노출되도록 익스플로러에서 설치 요구를 하며, 감염된 PC에서 시스템에 존재하는 특정 개인정보를 빼가거나, 시스템 명령을 수행을 통해 악의적 행위를 하는 경우

ActiveX 컨트롤은 공격자가 웹 인터페이스를 통해 누구나 언제든지 실행할 수 있습니다.

그림 1 Object Tag 및 Script를 이용한 호출

```
<OBJECT ID="update" WIDTH=0 HEIGHT=0 CLASSID="CLSID:3E01A824-">
<PARAM NAME="nam" VALUE='12'>
</OBJECT>

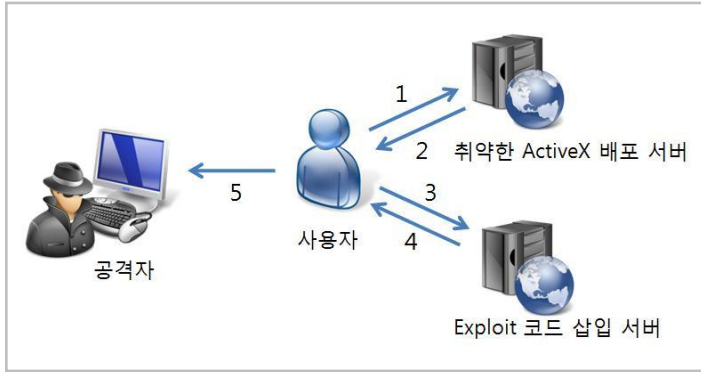
<script>

Update.Startupupdate()

</script>
```

ActiveX 취약점이 계속적으로 보고됨에 따라 많은 exploit 코드가 공개되고 있고 이 중에는 초보자들도 쉽게 활용할 수 있는 간단한 Exploit 코드들도 있습니다.

그림 2 ActiveX 취약점을 이용한 해킹 사례



1. 일반 사용자가 금융, 게임 등의 서비스를 이용하기 위해 취약한 ActiveX에 접근
2. 취약한 ActiveX를 설치하여 서비스를 이용
3. 일반 사용자가 XSS 취약점이 존재하는 웹 사이트나 게시판에 접근
4. XSS 취약점으로 인하여 Exploit 코드가 삽입된 악성 스크립트가 사용자의 PC에서 실행
5. 사용자의 PC에 대한 로컬 권한이 공격자에게 전달되어 공격자는 사용자PC의 로컬자원에 대한 제어 가능

ActiveX 컨트롤은 어느 사이트를 방문하더라도 ActiveX 설치를 강요 받습니다. 온라인 게임 설치 프로그램, 동영상 및 음악 플레이어, 공인인증서, 보안프로그램(키로거, 해킹방지, 온라인 백신, PC방화벽, 스파이웨어 등) 등에서 사용되고, 이는 거의 모든 국내 사이트에서 ActiveX 컨트롤이 사용되고 있습니다. RemoteCall 5 는 비 ActiveX 방식의 원격지원 서비스를 제공함으로 ActiveX의 취약점을 완벽히 차단합니다. 기존 RemoteCall v4.0 제품에서 ActiveX 방식의 원격지원을 서비스를 제공하였으나, 알서포트는 어떤 악의적인 코드를 삽입하지 않았으며, 알서포트의 ActiveX는 Object Tag와 스크립트를 사용하여 임의 호출하는 것에 대해 명령수행인자 (Parameter)를 사용하며, 여기에 사용되는 명령수행인자는 평문 (Text) 방식이 아닌 암호화된 명령수행인자를 사용함으로써 위 취약점을 완벽히 차단하여 제공하여 왔습니다.

알서포트에서 운영하는 사이트는 사전 취약점을 분석하여 보안패치 하여 운영하였으며, 지속적인 보안 취약점에 대한 모니터링과 패치를 수행하고 있습니다.

### 안전한 채널의 데이터 전송

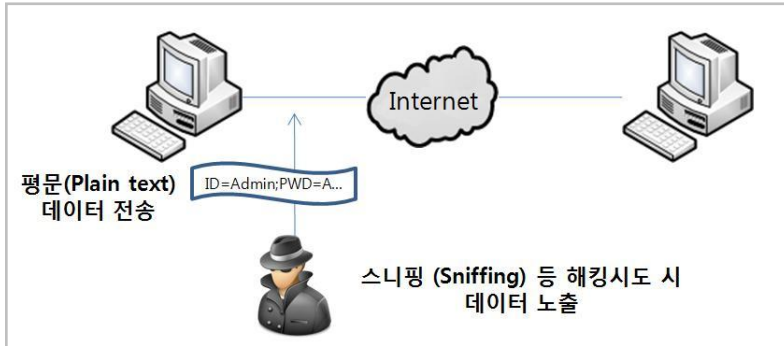
컴퓨터를 이용한 수많은 작업들은 로컬에 저장되거나, 인터넷을 통한 저장 과정을 거쳐 자료 축적이 이루어진다. 이러한 데이터는 네트워크를 통해 전송되면서 안전한 채널을 필요로 합니다.

평문 (Plain text)를 암호화 처리 없는 네트워크를 통한 데이터 전송은 해커들에 의한 스니핑 (Sniffing)



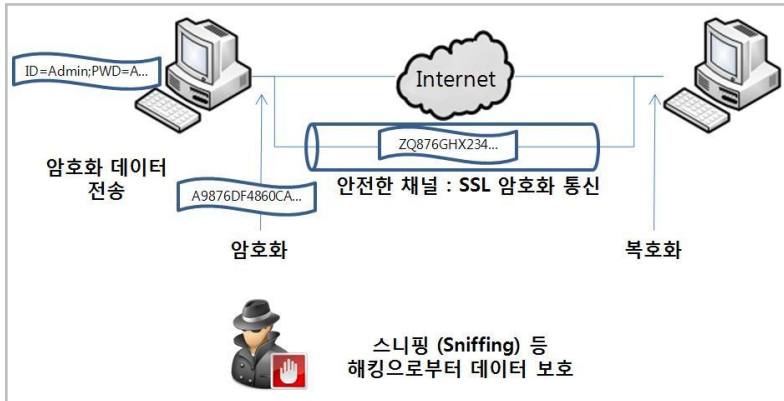
을 통해 해커에게 고스란히 노출될 위험이 있습니다.

그림 3 스니핑을 통한 해킹 시도 시 데이터 노출



안전한 채널의 데이터 전송을 위해서는 로컬에서 1차 암호화를 통하여 전송될 데이터에 대한 보안 처리를 거치고, 네트워크를 통한 데이터 전송의 경우 안전한 채널인 SSL (Secure Socket Layer) 암호화 통신을 통해 암호화된 채널을 사용하여 해커로부터 안전하게 보호할 수 있습니다.

그림 4 스니핑 등 해킹으로부터 데이터 보호



원격 원격지원시 보호되어야 할 데이터는 다음과 같습니다.

화면 공유 데이터, 키보드/마우스 컨트롤 데이터, 문자 채팅(Text Chat) 데이터, 파일 송수신 데이터, 기타 원격지원시 사용하는 기능에 의해 생성되는 데이터 등이 있습니다.

알서포트의 원격지원 제품은 End-To-End에서 256-bit AES 데이터 암호화를 통해 1차 데이터 보안 과정을 거칩니다.

원격지원 세션이 연결될 때 128-bit SSL (Secure Socket Layer) 암호화 통신을 통해 2차 보안 과정을 통해 안전한 채널을 유지합니다.

### 데이터 센터의 그리드 서버 보안

전 세계 데이터 센터에 알서포트의 그리드 서버를 구성하고 운영, 관리합니다. 현재, 알서포트의 그리

드 서버는 대한민국, 일본, 미국, 영국, 싱가포르의 데이터 센터에 위치하고 있습니다. 각 위치 데이터 센터는 24(hour) x 7(date) x 365(day) 직원이 운영, 관리를 받고 있으며 출입통제 보안은 생체인식 보안 시스템으로 보호 되고 있습니다. 그리드 서버는 서버 이중화를 통해 Active Standby로 상시 운용되고 있습니다.

## 웹 서버 보안

알서포트의 보안서버는 Thawte(www.thawte.com)으로부터 발급받은 SSL 웹 서버 인증서를 사용합니다. 원격지원 세션 연결 시 강력한 128-bit SSL (Secure Sockets Layer) 암호화 통신을 제공합니다. SSL (Secure Sockets Layer) 웹 서버 사용으로 PC와 서버 사이에 오가는 모든 데이터에 대해서 암호화 통신을 제공함으로써 악의적인 공격자의 스니핑(Sniffing) 공격에도 해독이 불가능한 안전한 데이터 전송을 합니다.

## 암호화 통신 지원

모든 지원 세션은 128bit SSL (Secure Socket Layer) 암호화 통신을 사용합니다.

## End-To-End 데이터 보호

모든 지원 세션에서 전달되는 데이터는 End-To-End에서 128-bit AES (Advanced Encryption Standard) 압축 암호화 전송합니다.

## 원격지원 접속 페이지(startsupport.com, rsup.net) 보안

모든 원격지원 세션은 startsupport.com 또는 rsup.net 접속페이지에서 다른 사용자들의 원격지원 리스트를 표시하지 않습니다.

## 원격지원 접속 코드 보안

원격지원 인증에 사용되는 접속코드는 랜덤 숫자인 6~9자리 숫자로 제공됩니다. 생성된 접속코드는 실제 통화(또는 채팅) 중인 상담원과의 원격지원 연결을 위해 1회 생성되고 사용됩니다. 일회성 원격 지원을 위해 사용되고, 제 3자의 임의 접근을 차단합니다.

## 안전한 HTTPS 통신 보안

사이트 접속 시 HTTPS를 지원합니다. HTTPS 통신을 통한 안전한 웹 접근을 제공합니다. SSL 암호화 세션 연결 시 443 Port 통신을 합니다.

## 원격지원 모듈의 전자서명과 코드사이닝 보안

전자서명(Digital Sign) 또는 코드사이닝(Code Signing)된 ActiveX 또는 Executable File를 사용합니다. Verisign에 의한 전자서명 또는 코드사이닝 인증된 모듈을 제공합니다.

## 비 ActiveX 방식의 원격지원

알서포트의 제품은 비 ActiveX 방식의 원격지원을 제공합니다. 채팅을 통해 상담을 시작할 수 있으며, 채팅을 통해 원격지원을 시작합니다. ActiveX 설치가 필요 없는 원격지원 서비스입니다.  
(구 버전인 RemoteCall v4.0 제품은 ActiveX 방식의 원격지원을 제공합니다.)

## No Pre-installed Software

원격지원을 받는 고객은 프로그램 설치 없이 즉시 익스플로러에서 쉽게 원격지원으로 받을 수 있습니다.

## 보안장비 호환

Firewall, IPS, HTTP Proxy 등 의 보안장비와 완벽하게 호환성을 유지합니다. 80 Port 의 HTTP 통신의 경우 80 Port로 통신하며, HTTPS 통신은 443 Port 통신을 함으로 방화벽 등 기타 보안장비의 환경변화가 필요 없습니다.

## 원격지원 사용자 사전 동의서

원격지원을 받는 고객은 상담원에게 원격지원 받기 위해 제어 권한에 대한 사전동의를 받은 후 화면 공유 및 지원이 시작됩니다.

## 원격지원시 키보드/마우스 제어권한 동의

원격지원을 받는 고객은 상담원에게 키보드, 마우스 제어에 대한 권한에 대한 사전 승인을 통한 화면 공유 및 지원이 시작됩니다. 원격지원 세션간에 언제든지 상담원에게 허락한 키보드/마우스 제어 권한을 회수할 수 있습니다. 키보드/마우스 제어 중단 기능은 "Ctrl + Alt + Shift" 키로 권한 회수가 가능합니다.

## 파일 송수신 고객 동의

파일 송수신 기능은 반드시 고객이 송수신 동의 과정을 필요로 합니다. 고객동의를 고객만이 확인 할 수 있습니다. 고객의 동의 없이 임의 파일 송수신을 안전하게 차단합니다.

## 원격지원 세션에 대한 Notification

원격지원 시작과 세션간에 원격지원 서비스를 이용에 대해 2가지를 제공합니다. "상담원이 원격지원 중입니다." 접속안내 창이 나타납니다. 고객은 언제든지 원격지원 종료 버튼으로 세션을 종료할 수 있습니다. 그리고, 고객의 데스크톱화면 오른쪽 하단에 "원격 지원 중"이라는 메시지가 항상 표시됩니다. 고객은 원격지원이 진행 중임을 인식할 수 있습니다.

## History Logging

채팅 및 파일 송수신시 주고 받았던 모든 기록은 로그로 기록되며, 서버로 전송되어 안전하게 관리됩니다. 원격지원 세션 레코딩은 상담원과 고객 모두 안전한 원격지원을 보장합니다.

## 간접제어 방식의 원격지원

마우스/키보드 직접제어를 제한하여 레이저포인터, 그리기 도구를 통한 상담원의 안내 및 사용법 지시를 합니다. 간접제어만으로 원격지원을 하여 직접제어에 의한 거부감 없이 안전한 원격지원을 제공합니다.

URL 전송 기능으로 직접제어를 하지 않고 웹사이트 안내를 할 수 있는 간접지원을 제공합니다.

### 원격지원시 사용된 모듈의 로컬 Uninstall

원격지원 종료 후 고객 PC의 원격지원 모듈을 모두 삭제할 수 있습니다.

### 상담원의 모든 기능에 대한 중앙통제

대부분의 주요 기능은 관리자에 의하여 중앙 통제를 할 수 있습니다. 관리자는 상담원의 권한을 등급별로 직접제어 권한 또는 간접제어 권한 부여를 할 수 있습니다.

### 상담원 PC의 접속 IP 또는 Mac Address 접근 통제 설정

관리자는 허가하는 상담원의 네트워크 또는 장비의 위치를 제한할 수 있습니다. 관리자는 관리페이지에서 지정 IP 또는 IP 그룹, Mac Address 를 설정 등록하고, 사용자는 허용되는 위치에서 뷰어 로그인 후 상담을 시작할 수 있습니다.

## Appendix

### SSL (Secure Socket Layer)

SSL 은 응용 프로토콜 TCP/IP 사이에 위치하며, 데이터의 암호화, 서버의 인증, 메시지의 무결성을 제공해 준다. 서버에 대한 인증은 반드시 수행되지만 클라이언트에 대한 인증은 선택적으로 수행할 수 있도록 합니다.

SSL은 서버와 클라이언트 양쪽의 TCP/IP 연결을 위하여 핸드셰이크 (handshake) 프로토콜을 수행한다. 이 결과로 양쪽은 암호화 통신에 합의하고, 암호화 통신과 인증에 필요한 값들을 준비합니다.

이 단계가 지나면 SSL은 응용 프로토콜에서 생성해 낸 바이트(Byte) 스트림의 암호화와 복호화만 수행하게 됩니다. 이는 HTTP 요청(Request)과 HTTP 응답(Response)에 포함되는 정보들이 암호화되어 전송된다는 것을 의미합니다.

### AES (Advanced Encryption Standard)

AES(Advanced Encryption Standard)는 2001년 미국 정부에서 채택한 암호화의 형식입니다. AES는 이전의 DES(Data Encryption Standard), 3DES보다 훨씬 안전한 암호화를 제공합니다.

**RSUPPORT**

**Product information**  
<http://www.rsupport.com>

**Sales inquiries**  
sales@rsupport.co.kr  
02-479-4430

**Media inquiries**  
mkt@rsupport.co.kr  
070-7011-1402

For more information on  
RemoteCall, please visit  
<http://www.rsupport.com>