Wherever possible
RSUPPORT

Security white paper

RSUPPORT

http://www.rsupport.com

For more information, please visit us online.

Carbonless Support
Microsoft GOLD CERTIFIED Partner
Compatible with Windows 7
intel

Go Secure with RSUPPORT

Introduction

RSUPPORT's products are remote support tools that anyone from regular users to professionals can use to give and receive remote support; connecting with each other via their browser.
RSUPPORT's products provide a secure remote support environment.

Is ActiveX Vulnerable?

ActiveX was announced in the beginning of 1996, known as an extension of the COM (Component Object Model), it is now being integrated with .NET through the DCOM (Distributed COM). ActiveX was announced as an alternative of SUN's JAVA. OLE (Object Linking and Embedding) technology which could be called Microsoft's revolution of the API, means the Objects linked with OLE could be applicable and executable along with the other application.

ActiveX is based on the trust model. MS uses this method to permit only signed ActiveX controls, not unsigned ActiveX controls. It executes when the Signed ActiveX control doesn't contain any malicious code.

Known security vulnerability for ActiveX controls:

1. Provides a method to directly access local resources.
2. Malicious behavior using auto-update to distribute unintended files.
3. Bypass logic algorithms using forged input values.
4. Buffer overflow vulnerability for Method or Property input values.
5. Malicious behavior that executes malicious code (i.e., Black ActiveX) through a vulnerability in a website. Requiring everyone who visits the site with IE to install it. This can be used to steal private information from the infected PC and run malicious system commands.

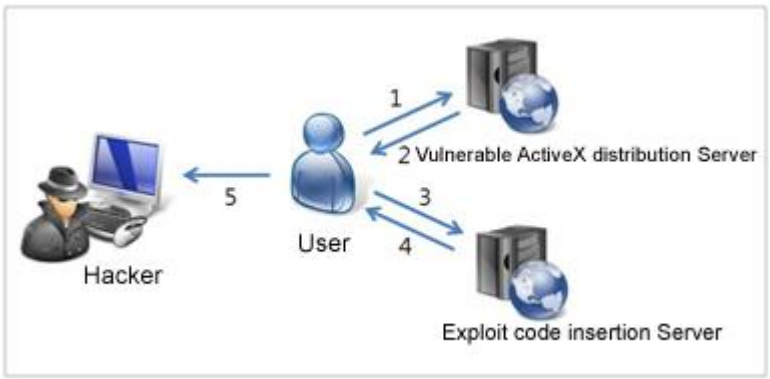
An ActiveX control could be executed by hackers to attack anyone through a web interface.

Image 1 Calls using Object Tag and Script

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

<script>

Update.Startupdate()

</script>
```

As ActiveX vulnerabilities keep being reported, a lot of exploited code is open to the public. There are many simple code exploits easily available on the Internet today.

Image 2 Hacking using ActiveX vulnerability



1. Access to a vulnerable ActiveX control used for a service such as online banking.
2. Installing a vulnerable ActiveX control.
3. Access to a website or bulletin board that has an XSS (Cross Site Scripting) vulnerability.
4. A malicious script exploit is executed on the computer through the XSS vulnerability.
5. A hacker can control the resources on the remote computer because the hacker has local privileges on the user's computer.

You are required to install an ActiveX control for most interactive websites these days. It is used for online gaming, installation programs, movie/music players, public certificates, security programs (Key logger, Hacking protection, Online vaccine, PC Firewall, Spyware etc.). RemoteCall 5.0 protects against ActiveX vulnerabilities by providing a non-ActiveX remote support system. Even though RSUPPORT used ActiveX in the previous version of RemoteCall,
there was no malicious code and use Parameters for arbitrary calling using Object Tag and Script. Also, these parameters are encrypted to protect against security vulnerabilities.

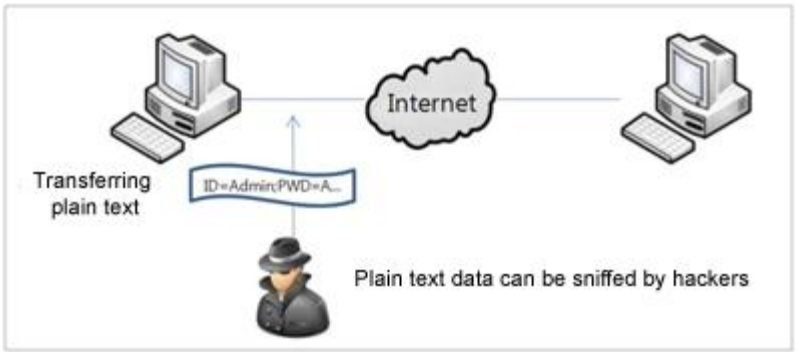
All RSUPPORT websites consistently analyze and patch against possible vulnerabilities, as well RSUPPORT continuously monitors and patches security vulnerabilities as they come up.

Data Transfer through a Secured Channel

Data (both work and personal content) is stored on local computers or online via the Internet. This data requires a secured channel for file transferring.

Transferring unencrypted plain text data can be picked up by hackers anytime, anywhere.

Image 3 Data exposure by sniffing



To transfer secure data and protect it from hackers, data should be encrypted on the local computer first and make use of an encrypted channel such as SSL (Secure Socket Layer) to send it over the network.

Image 4 Data protection from hacking (network sniffing)

The below data should be protected while supporting the remote computer:
Screen Sharing, Keyboard/Mouse control, Text Chat, File Transfer, data created by remote support functions.

RSUPPORT's products support 256-bit AES end-to-end encryption as a first line of defense.
128-bit SSL (Secure Socket Layer) is involved during the remote session as a secondary security process.

Grid Server security at the Data Center

RSUPPORT is operating and managing grid servers in Data Centers all over the world.
RSUPPORT currently has grid servers in Korea, Japan, USA and Singapore. Each data center is managed and operated by local staff 24/7 and secured by biometrics entrance security systems. The grid servers support zero downtime failover processes.

Web Server Security

RSUPPORT's servers utilize SSL web server certificate issued by Thawte (www.thawte.com). This enables RSUPPORT to provide secure 128-bit SSL (Secure Sockets Layer) encryption during the support sessions.
While using SSL (Secure Sockets Layer) on the web server, all data and information between PC and server can be secured and transferred without the risk of network sniffers intercepting the data.

End-To-End Encrypted Connections

Every support session uses 128-bit end-to-end SSL (Secured Socket Layer) encryption.

High Level Data Encryption

Every support session uses 256-bit end-to-end AES (Advanced Encryption Standard) encryption for all transferred data.

Support Page (startsupport.com, rsup.net) Security

The shared support pages (e.g., http://startsupport.com and http://rsup.net) do not display any personal information to the public.

Connection Code Security

Connection Codes used for remote support authorization provide a 6 to 9 digit random number to the customer. Generated connection codes are disposed of after the support session has started. Another user cannot connect to the same session once it was been established.

Secure HTTP (HTTPS)

The support pages use HTTPS for encryption. Users can safely access these pages and enter their contact information. HTTPS uses port 443 for communication.

Digital Signature and Code Signing for Remote Support Module

RSUPPORT uses digitally signed or code signed ActiveX and/or Executable files which are digitally signed and verified by VeriSign (www.verisign.com).

Non ActiveX Remote Support

RSUPPORT also provides a non ActiveX remote support connection method. The new products initiate support or screen sharing through a web based chat window which does not require any files to run or install. Screen sharing and remote control is accomplished by running a one-time executable file (.exe).

No Pre-Installed Software

The customer is able to initiate a remote support session without installing or running any files.

Security Equipment

RSUPPORT's products are completely compatible with standard security equipment such as Firewalls, IPS, and HTTP Proxy. They use port 80 for HTTP and port 443 for HTTPS. In most cases, Port 443 and 80 are available to end users since these 2 ports are network standards.

User authorization to initiate remote support

Customers must authorize the representative to share their desktop before initiating remote support.

User authorization for Keyboard/Mouse control

Mouse/Keyboard control needs to be approved by the customer before the support session begins. Customer can regain Keyboard/Mouse control at any time by simple moving their mouse or pressing "Ctrl + Alt + Shift".

User authorization for File Transfers

File transfers must also be authorized by customers before the representative can send a file to the customers computer, or download a file from their computer.

Notification of the active support session

The customer is notified in two ways that they are currently in a remote support session. One is a connection status window that shows connection information which users can use to disconnect the session at any time. The other is the on-screen message in the bottom-right corner of the desktop displaying "Screen Sharing...".

Session Logging

Chat and file transfer sessions leave behind logs saved to the session server. Remote support session logging ensures safe remote support for both users and representatives.

Indirect control for remote support

The laser pointer and on-screen drawing enables representatives to support the customer without taking full control of their keyboard and mouse. These indirect support tools give the customers peace of mind during the session. URL push is also an indirect remote support tool which can be used to direct users to specific websites without actually opening their browser for them.

Zero Footprint Post Session

Customers can remove the entire support module after the session has ended, leaving no trace of the session on their system.

Permissions for representative control

RSUPPORT products provide an Administrators with a powerful Admin Center where permission settings may be applied to individual support representatives to restrict access and control. Administrators can also group representatives together and apply group permission settings.

Network Restrictions

Network access restrictions are provided for Administrators to restrict access to the application by IP and MAC address. Administrators can insure that the support representatives can only access the program while in the local office network and not from their private residence.

Appendix

SSL (Secure Socket Layer)

SSL is placed between the Application protocol and TCP/IP and provides data encryption, server authentication, and insures the integrity of messages. Server authentication is mandatory but client authentication is optional.

SSL performs a handshake protocol to connect the server and client with TCP/IP. This results in bilateral encryption and prepares the necessary values for encryption correspondence and authentication.

After this step, SSL performs encryption and decryption of the Bytes that the application protocol generates. This means all information including the HTTP requests and HTTP responses are encrypted and transferred.

AES (Advanced Encryption Standard)

AES(Advanced Encryption Standard) is an encryption algorithm that the US Government adopted in 2001. AES provides a higher level of secured encryption than DES (Data Encryption Standard) or 3DES.

Wherever possible
RSUPPORT

For more information about RSUPPORT, please visit **http://www.rsupport.com**

Korea :

(138-724) 서울시 송파구 방이동 45번지
한미타워 15층, 16층
전 화 : +82-70-7011-3900
팩 스 : +82-2-479-4429
기술문의 : support.kr@rsupport.com
구매문의 : sales.kr@rsupport.com
기타문의 : info.kr@rsupport.com

Japan :

〒100-0013 東京都千代田区霞ヶ関3-3-2
新霞ヶ関ビル18階KOTRA
TEL : +81-3-3539-5761
FAX : +81-3-3539-5762
お問い合わせ : support.jp@rsupport.com
Sales : sales.jp@rsupport.com
Info : info.jp@rsupport.com

USA :

333 Sylvan Avenue Suite 110,
Englewood Cliffs, NJ 07632
Phone : +1-888-348-6330
Fax : +1-888-348-6340
Tech : support.us@rsupport.com
Sales : sales.us@rsupport.com
Info : info.us@rsupport.com

China :

北京市朝阳区霄云路38号
现代汽车大厦2203室I-101
电话 : +86-10-8256-1810
传真 : +86-10-8256-2978
支持咨询 : support.cn@rsupport.com
业务咨询 : sales.cn@rsupport.com
销售咨询 : info.cn@rsupport.com