

## QuickTime Vulnerability Exposed by Contest Poses Wide Risk

Rich Mogull, Greg Young

All Java-enabled browsers with Apple QuickTime installed are at risk from a vulnerability discovered at a security conference contest. The incident highlights the danger of vulnerability research conducted in public.

## NEWS ANALYSIS

---

### Event

- On 20 April 2007, at a Macintosh hacking contest held at and conducted by the CanSecWest security conference in Vancouver, two security researchers successfully broke into a MacBook Pro notebook computer with all currently available security patches installed. For this exploit, the researchers collected a \$10,000 prize offered by the intrusion prevention system (IPS) vendor TippingPoint (a division of 3Com), and the MacBook Pro.
- On 23 April 2007, researchers discovered that the flaw exists in Apple QuickTime player, and that any system with a Java-enabled browser and QuickTime installed is potentially vulnerable to attack — including Safari, Mozilla's Firefox and Microsoft Internet Explorer — if it is installed on the Mac or Windows operating systems. No patch is yet available.

### Analysis

Although there are no confirmed reports of any exploits for this vulnerability, with some details of the vulnerability now public, enterprises should assume they are at risk for a potential breach.

Upon further investigation, researchers found that the vulnerability lies within an application programming interface (API) that QuickTime exposes to Java applets (code run in Web browsers). A successful exploit would provide access at the privilege of the currently logged-in user. So far, the vulnerability is known to affect any Web browser on any operating system with QuickTime 2 installed and enabled in the Web browser. The sheer breadth of systems and browsers that potentially could be affected means that this could be a serious browser vulnerability. No single safeguard can guarantee complete protection.

Public vulnerability research and "hacking contests" are risky endeavors, and can run contrary to responsible disclosure practices, whereby vendors are given an opportunity to develop patches or remediation before any public announcements. Vulnerability research is an extremely valuable endeavor for ensuring more secure IT. However, conducting vulnerability research in a public venue is risky and could potentially lead to mishandling or treating too lightly these vulnerabilities — which can turn a well-intentioned action into a more ambiguous one, or inadvertently provide assistance to attackers.

### RECOMMENDATIONS

---

#### Users:

- Weigh the loss of functionality and disruption of disabling Java and/or removing QuickTime 2 until Apple (and possibly browser makers) makes a patch available, against the fact that, as yet, there have been no known exploits and some protection via other safeguarding is available.
- If you use host IPSs, download the specific signature as a safeguard when it becomes available, since an exploit could be conducted via Web mail, or while a user is outside the enterprise perimeter (for example, on laptops). Look for signatures from your vendor for this vulnerability when they become available. Update antivirus signatures for e-mail-

based applications when they become available, as they could assist with protecting against an e-mail vector.

- Enable network IPS signatures for this vulnerability as they become available to block potential attacks via Web links. Network IPSs offer a good first line of defense; however, recognize that an exploit could be made via an SSL encrypted session that is not subject to inspection.

#### **Vendors and security services firms:**

- Consider ending public vulnerability marketing events, which may lead to unanticipated consequences that endanger IT users.

#### **RECOMMENDED READING**

---

- "Responsible Vulnerability Disclosure: Guidance for Researchers, Vendors and End Users" — Responsible disclosure means that the researcher and vendor work together diligently and ethically to produce a timely patch to reduce the risk as much as possible for end-user organizations. **By Amrit Williams, John Pescatore and Paul Proctor**
- "Best Practices for Network Vulnerability Assessment" — The value of vulnerability assessment to an organization depends on the deployment methods and the internal processes in place to act on the report data. **By Amrit Williams, Mark Nicolett and Kelly Kavanaugh**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

## REGIONAL HEADQUARTERS

---

### **Corporate Headquarters**

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

### **European Headquarters**

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

### **Asia/Pacific Headquarters**

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### **Japan Headquarters**

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### **Latin America Headquarters**

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509