



FIRSTLIGHT SIGNATURE SERVICE

SIGNATURE OF THE WEEK

February 22nd, 2008

SIGNATURE NAMES

```
SetBgColor.QTPlugin.Quicktime.ActiveX.Buffer.Overflow.A  
SetTarget.Quicktime.ActiveX.Buffer.Overflow.A  
SetHREF.QTPlugin.Quicktime.ActiveX.Buffer.Overflow.A  
SetMatrix.Quicktime.ActiveX.Buffer.Overflow.A  
SetMovieName.Quicktime.ActiveX.Buffer.Overflow.A
```

DESCRIPTION

Apple Quicktime is a widely used media player that plays a variety of different media formats and contains several browser extensions.

A stack overflow was discovered in the Apple Quicktime ActiveX control that could be used to execute arbitrary code on a vulnerable system. In order to exploit this vulnerability, an attacker would have to trick their victim into visiting a maliciously crafted web page. As of February 22nd, 2008, Apple has not released a patch to address this issue.

The Endeavor signatures will trigger on use of the vulnerable class identifier and method.

IMPACT

User Assisted Remote Code Execution

REFERENCES

<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-0778>
<http://www.milw0rm.com/exploits/5110>

DISCLOSURE DATE

February 13th, 2008

ENDEAVOR RESPONSE DATE

February 13th, 2008

The FirstLight Signature Service provides IPS, UTM, and Firewall vendors with a timely high quality signature set that is constantly being updated, revised and extended. The FirstLight signature set comprises over 12000 signatures that cover a broad range of both emerging and established threats.

Major areas covered by the FirstLight signature set include Client Side Attacks, Server Side Attacks, Exploit Components, Malware, Web Application Attacks, Protocols and Policy.

This document serves to notify our customers of the most important signature developed this week.