# CVE Detail – CVE-2008-3438

Apple Mac OS X does not properly verify the authenticity of updates, which allows man-in-the-middle attackers to execute arbitrary code via a Trojan horse update, as demonstrated by evilgrade and DNS cache poisoning.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.61697

## CVSS Scoring

CVSS v3.1 Score: 8.1

Severity: HIGH

## Mapped CWE(s)

* CWE-494: Download of Code Without Integrity Check

## CAPEC(s)

* CAPEC-184: Software Integrity Attack
* CAPEC-185: Malicious Software Download
* CAPEC-186: Malicious Software Update
* CAPEC-187: Malicious Automated Software Update via Redirection
* CAPEC-533: Malicious Manual Software Update
* CAPEC-538: Open-Source Library Manipulation
* CAPEC-657: Malicious Automated Software Update via Spoofing
* CAPEC-662: Adversary in the Browser (AiTB)
* CAPEC-691: Spoof Open-Source Software Metadata
* CAPEC-692: Spoof Version Control System Commit Metadata
* CAPEC-693: StarJacking
* CAPEC-695: Repo Jacking

## ATT&CK Techniques

* T1195.001: Compromise Software Dependencies and Development Tools
* T1185: Browser Session Hijacking
* T1072: Software Deployment Tools
* T1195.002: Compromise Software Supply Chain

## Used By (Actors/Tools)

* TrickBot (malware)
* Ursnif (malware)
* TRANSLATEXT (malware)
* IcedID (malware)
* Chaes (malware)
* Grandoreiro (malware)
* XLoader (malware)
* Wiper (malware)
* Cobalt Strike (malware)
* CCBkdr (malware)
* GoldenSpy (malware)
* Carberp (malware)
* SUNSPOT (malware)
* Melcoz (malware)
* XCSSET (malware)
* Agent Tesla (malware)
* QakBot (malware)
* Dridex (malware)
* FIN7 (intrusion-set)
* Dragonfly (intrusion-set)
* SolarWinds Compromise (campaign)
* Daggerfly (intrusion-set)
* Sandworm Team (intrusion-set)
* Silence (intrusion-set)
* Cobalt Group (intrusion-set)
* APT32 (intrusion-set)
* Kimsuky (intrusion-set)
* C0018 (campaign)
* Threat Group-1314 (intrusion-set)
* APT41 (intrusion-set)
* Threat Group-3390 (intrusion-set)
* Moonstone Sleet (intrusion-set)
* GOLD SOUTHFIELD (intrusion-set)

## Affected Products

* cpe:2.3:o:apple:mac\_os\_x:\*:\*:\*:\*:\*:\*:\*:\*