



Security Alert from the Office of the CTO

January 18, 2010

Operation Aurora - Google and 30 others attacked

What Happened & What To Do Now

McAfee issued a press release today offering guidance to help organizations determine if they were impacted by "Operation Aurora," a high profile cyberattack that has struck Google and a growing list of other companies. Since the full extent of this attack is not yet known, McAfee is taking steps to help customers understand what to do now in order to determine if you are susceptible to the vulnerability, and if so, how to prevent an attack or remediate the problem if you have been compromised.

We are working with multiple organizations that were impacted by this attack as well as the government and law enforcement. As part of our investigation, we analyzed several pieces of malicious code that we have confirmed were used in attempts to penetrate several of the targeted organizations.

Description of the attack

McAfee Labs identified a zero-day vulnerability in Microsoft Internet Explorer that was used as an entry point for "Operation Aurora" to exploit Google and at least 30 other companies. Microsoft has issued a security advisory and McAfee is working closely with them on this matter. "Operation Aurora" was a coordinated attack which included a piece of computer code that exploits a vulnerability in Internet Explorer to gain access to computer systems. This exploit is then extended to download and activate malware within the systems. The attack, which was initiated surreptitiously when targeted users accessed a malicious Web page (likely because they believed it to be reputable), ultimately connected those computer systems to a remote server. That connection was used to steal company intellectual property and, in Google's case, gain access to user accounts. [Learn more.](#)

What is McAfee doing to protect customers?

Researchers at McAfee Labs are delivering signature updates, product configuration suggestions, and advice on a continuous basis on the [McAfee Labs blog](#).

1. Helping customers understand if they have been infected

Aurora, for the known attacks to date, delivers a set of files and utilizes a set of external domains in its attacks. Analyzing your systems and infrastructure for these identifiers can indicate exposure. McAfee offers vulnerability and risk assessments to pinpoint which assets and data may be at risk within your environment. Below is a summary of McAfee's assessment of Microsoft Internet Explorer platform risks:

Platform	IE 6 Vulnerable	IE 7 Vulnerable	IE 8 Vulnerable
Windows 2000	High Risk	N/A	N/A
Windows XP	High Risk	High Risk	Medium Risk (DEP Enable SP3)
Windows 2003	Medium Risk (Dep Enable)	Medium Risk (Dep Enabled)	Medium Risk (Dep Enabled)
Windows Vista	N/A	Medium Risk (Protected Mode)	Medium Risk (DEP Enabled with SP1)
Windows 2008	N/A	N/A	Medium Risk (DEP Enabled)

Windows 7	N/A	N/A	Medium Risk (DEP Enabled)
-----------	-----	-----	------------------------------

2. Recommending upgrades to protect customer systems

McAfee is recommending all customers upgrade their system protection by downloading the latest security intelligence:

- a. Ensure your McAfee antivirus/antimalware is up to date with a .DAT file 5862 or greater.
- b. Run a full system scan on each system if your .DAT files were not at this level.
- c. Enable Artemis, McAfee's real-time file reputation engine which protects against known, new, and emerging threats, on your endpoint products. If you do not know how to do this, please visit the [McAfee Corporate Knowledge Base](#) to access a video tutorial.
- d. Turn your browser security setting to HIGH and restrict browsing to known sites until Microsoft provides a patch for the Internet Explorer exploit.
- e. If you have the capability to log all outbound Web requests, do so for future forensics.

3. Remediating customer systems that have been compromised

If a customer believes or discovers they have been infected by Aurora, McAfee is offering onsite Incident Response Services to qualified companies.

4. Preventing new attacks from impacting customers

McAfee has several solutions to prevent Aurora from having any impact to customers systems, network and data. From VirusScan Enterprise, to Intrusion Prevention, Firewalls, and Application Whitelisting, McAfee has a host of solutions.

5. Providing online real-time resources

McAfee's free [Support Notification Service](#) to get the latest critical alerts, notices, and bulletins
McAfee Labs [Security Advisories](#)
McAfee Worldwide CTO George Kurtz's [blog](#)
McAfee Labs [blog](#)
Learn more about McAfee Labs [Global Threat Intelligence](#)

We will continue to provide updates on this event as it continues to unfold. As I [said in my last post](#), this is only the tip of the iceberg.

To get real time updates on this story follow me on Twitter at http://www.twitter.com/george_kurtzCTO

Regards,

George Kurtz
Worldwide Chief Technology Officer and Executive Vice President
McAfee