MICROSOLVED,INC.

2330 Briggs Road
Columbus, OH 43223

T 614-351-1237
F 614-351-9015
info@microsolved.com

www.microsolved.com
stateofsecurity.com

This is a summary risk assessment for an emerging threat on the public Internet. Please contact us if you have any questions or would like assistance with any issues stemming from this security issue.

CVE-2009-1136 Office Web Components Vulnerability Risk Assessment

Overview:

A “0-Day” Active-X vulnerability that could lead to code execution is spreading on the public Internet.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1136

Vectors:

1. Internet Explorer, via a malicious page without user interaction

2. Email, embedded attack code, Outlook requires user interaction to exploit

3. Email as attachment, opening a spreadsheet causes exploitation

Scope:

Attack is actively being exploited in the wild.

Exploit and toolkits are available. (MetaSploit, etc.)

Non-Windows systems not exploitable

Some Windows server OS loads not exploitable

Attack Prerequisites:

None needed, mass delivery possible

Threat Agent Coverage:

Widely available exploit code means wide scale adoption by all of the attacker spectrum

Focused attackers waiting for a 0-day may now have a window of opportunity to act and be able to hide in the "script kiddy" noise, or use this simply to gain a beachead, knowing that cleanup will occur, but then digging in via other means to establish long term compromise (this is not the standard mathamatically probable attack model)

Risk Ratings:

Workstation Risk: **HIGH*

Probability: High - active wild exploitation, likely worm/bot evolution

Impact: Medium - exploitation gains command context of user, administrator/system context would require additional exploitation if best practices are in place

Server Risk: **LOW*

Probability: Low - if best practices are in place, users should not be using any of the attack vectors on a server platform, risk to servers is mostly the result of compromised victim workstations

Impact: Low - Little impact issue outside of normal server level risk that user compromises could be leveraged against the infrastructure

Overall Enterprise Risk: **Medium*

Given an environment with best practices in place, compromise of a set of workstation systems is always likely, but is accounted for in their risk posture. However, given the ease of exploitation on the workstation side and the possibility of introducing longer-term attackers with increased capabilities beyond the day-to-day threat levels, additional risk is created. While the probability of short term threats to protected data is elevated, longer term threats from this event should be mitigated by proper security practices. Impact should remain consistent, thus the medium rating of enterprise risk.

Mitigating Controls:

Setting kill bits for Active X web office components in IE

Not using a browser with Active X controls

Contributing Controls:

Domain blocks for known malware hosting domains, though minimally capable due to entropy in the malware hosts

Anti-virus signatures, where available, minimally effective as attackers can modify the payload to avoid heuristic detections (useful to stop basic attackers and most automated platforms)

NIDS to detect the exploit and possibly prevent infection (unlikely to be effective against anything more than basic attacks)

Suggested Mitigation Strategy:

Short Term:

Organizations should deploy the kill bits specified by Microsoft in this article:
http://www.microsoft.com/technet/security/advisory/973472.mspx

Individuals can apply the self fix in this article: http://support.microsoft.com/kb/973472

AV signatures should also be updated frequently in the short term to ensure coverage as the signatures become available.

Network blocking of known malware domains in content filers, NIDS and other defense tools should also be updated frequently over the next 96 hours to ensure up to date coverage as much as possible.

Steps to educate users about this threat and the potential dangers of office documents should be undertaken as soon as possible.

Long Term:

Organizations should take steps to ensure that their risk postures allow for potentially compromised end-user systems and that their networks are engineered and capable of detecting such attacks. Assessments to ensure best practices compliance should be ongoing.

Organizations should consider replacing Internet Explorer as the default browser, or at least offering non-IE browsers as an alternative to their user population. This reduces the vulnerability footprint of browsing that is exploited on a routine basis in a majority of browser-focused attacks.