US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
August 25, 2008
Volume 3, Issue 3

# QUARTERLY TRENDS AND ANALYSIS REPORT

www.us-cert.gov

## Introduction

This report summarizes and provides analysis of incident reports submitted to US-CERT during the U.S. Government fiscal year 2008 third quarter (FY08 Q3), which is the period of April 1, 2008 to June 30, 2008.

US-CERT is a partnership between the Department of Homeland Security (DHS) and the public and private sectors. Established in 2003 to protect the nation's internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. The organization interacts with federal agencies, state and local governments, industry professionals, and others to improve information sharing and incident response coordination and to reduce cyber threats and vulnerabilities.

US-CERT provides the following support:

- 24 x 7 x 365 triage support to federal, public, and private sectors, and the international community
- cyber security event monitoring and predictive analysis
- advanced warning on emerging threats
- incident response capabilities for federal and state agencies
- malware analysis and recovery support
- trends and analysis reporting tools
- development and participation in national and international level exercises

## INSIDE THIS ISSUE



The purpose of this report is to provide awareness of the cyber security trends as observed by US-CERT. The analysis in this report is based on incident information that has been reported to US-CERT, incidents identified by US-CERT, and public/private sector information identified when correlating and analyzing the data. A computer incident within US-CERT is, as defined by NIST Special Publication 800-61, a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

This report also provides information on notable security topics and trends, including emerging threats and updates to topics discussed in previous issues.

# Cyber Security Trends, Metrics, and Security Indicators

US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to collect reasoned and actionable cyber security information and to identify emerging cyber security threats. Based on the information reported, US-CERT was able to identify the following cyber security trends for fiscal year 2008 third quarter (FY08 Q3).

The definition of each reporting category is delineated in Table 1 shown below.

| Category | Description |
|---|---|
| **CAT 1** Unauthorized Access | In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource. |
| **CAT 2** Denial of Service (DoS) | An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS. |
| **CAT 3** Malicious Code | *Successful* installation of malicious software (e.g., virus, worm, spyware, bot, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application). Agencies are *not* required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software. |
| **CAT 4** Improper Usage | A person violates acceptable computing use policies. |
| **CAT 5** Scans, Probes, or Attempted Access | Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. |
| **CAT 6** Investigation | *Unconfirmed* incidents of potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. |

Figure 1 displays the overall distribution of cyber security incidents and events across the six major categories described in Table 1.

The proportion of Category 5 reports increased 3.2% from the previous quarter.

**Figure 1: Incidents and Events by Category**

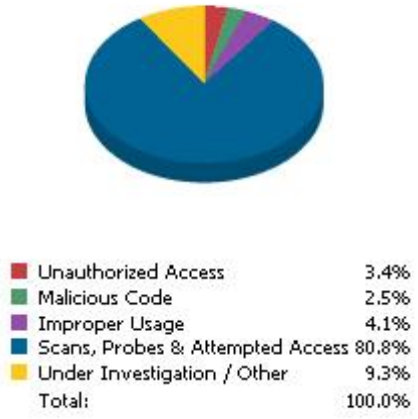


Figure 2 is a breakdown of the top five incidents and events versus all others. The top incident type reported to US-CERT was phishing, accounting for just over 76% of all incidents reported.

US-CERT encourages all users and organizations to report any activities that you feel meet the criteria for an incident. To learn more about incidents, visit https://forms.us-cert.gov/report/. To report phishing, visit http://www.us-cert.gov/nav/report_phishing.html.

**Figure 2: Top Five Incidents vs. All Others**

# Debian and Ubuntu OpenSSL Random Number Generator Vulnerability

On May 13, 2008, Debian and Ubuntu released multiple security advisories to address a vulnerability in the random number generator used by the OpenSSL package included in the Debian GNU/Linux operating system and its derivatives. The vulnerability causes predictable cryptographic keys to be generated by any application that uses the affected versions of the OpenSSL package. Exploitation of this vulnerability could allow a remote, unauthenticated attacker with minimal knowledge of the vulnerable system and the ability to conduct a brute force attack against an affected application, to guess secret key material. Secondary impacts include authenticated access to the system through the affected service or the ability to perform man-in-the-middle attacks.

Vulnerable keys include the following:

- SSH keys
- OpenVPN keys
- DNSSEC keys
- Key material used in X.509 certificates
- Session keys used in SSL/TLS connections

In addition, Digital Signature Algorithm (DSA) keys generated for digital signing and authentication should also be considered compromised. Any keys generated using the affected systems on or after September 17, 2006, may be vulnerable. Please note that keys generated with GnuPG or GNUTLS on the affected systems are not vulnerable because these applications use different random number generators from the flawed version of OpenSSL.

US-CERT updated Current Activity on the website (www.us-cert.gov) and recommended that users apply the patch from the vendor and regenerate key material. More information regarding this vulnerability can be found in US-CERT Vulnerability Note, VU#925211. Additional instructions for generating new keys can be found at http://www.debian.org/security/key-rollover/.

# DNS Cache Poisoning Vulnerability

DNS servers employ caches of memory to improve their performance when answering multiple identical queries. When a DNS server answers a query with information that did not originate from an authoritative DNS server, it is considered poisoned. DNS cache poisoning (sometimes referred to as cache pollution) is an attack technique that allows an attacker to introduce forged DNS information into the cache of a caching nameserver. Due to the caching mechanism, a poisoned DNS server will continue to answer queries for the forged information until the cached answer times out.

A successful cache poisoning attack can cause a nameserver's clients to contact the incorrect, and possibly malicious, hosts for particular services. This may allow an attacker to obtain sensitive information or mislead users into believing they are visiting a legitimate website. Technical details regarding this vulnerability have been posted to public websites. Attackers could use these details to construct exploit code. Users have been encouraged to patch systems or apply workarounds immediately.

US-CERT first reported on this on July 8, 2008, after multiple vendors released updates to resolve weakness in DNS implementations that could leave vulnerable systems open to cache poisoning. These patches implement source port randomization in the nameserver as a way to reduce the practicality of cache poisoning attacks. US-CERT released Vulnerability Note VU#800113 and a Current Activity entry to detail the vulnerability and provide mitigation strategies.

# Phishing and Spamming Trends

A number of notable trends were identified this quarter in "State of Spam" reports issued on a monthly basis by Symantec:

- Hacked personal email account used to scam contacts
- Spammers simplify email harvesting technique
- China earthquake tragedy used to spread viruses
- Olympics related lottery scam emerges
- Bogus news events lure innocent victims

The full reports can be viewed at: http://www.symantec.com/business/theme.jsp?themeid=state_of_spam#

***Other Notable Phishing Campaigns***

Researchers at VeriSign Inc. recently reported on the success of spear phishing tactics. The researchers tracked 66 spear phishing incidents dating back from February 2007 and discovered that two criminal organizations were responsible for 95% of the incidents and stole data from an estimated 15,000 victims.[1]

The most successful of these spear phishing attacks studied by VeriSign was launched in April 2008. CEOs were targeted with fake subpoenas that included their names, organizations, telephone numbers, and a link to download bogus legal documents. If the recipients clicked the link, they would be directed to a website and instructed to install a plug-in to view the documents. The plug-in was actually a type of malware, that if installed, the attackers could use to collect information from the compromised systems. The perceived threat of legal action was particularly effective in this campaign. US Courts released a statement regarding these spear phishing emails.[2]

Additionally, US-CERT released a Current Activity entry to warn users of this campaign and to provide recommendations to mitigate the risk. During the quarter, US-CERT also received public reports of a phishing campaign involving the US Tax Court. These messages contained very specific information about the recipients with a link to download additional information regarding a bogus petition.

If users clicked the link, they would be instructed to install a bogus root certificate falsely signed by "VeriSign Trust Network," then an ActiveX control falsely signed by "Adobe Systems Incorporated," which actually functions as an information stealer. By including specific information about the recipient and falsely using recognized organizations such as VeriSign, Adobe, and the US Tax Court, such a scam could be difficult to recognize.

In the past, US-CERT has received reports of an increased number of phishing scams following natural disasters. Due to recent natural disasters (e.g., Myanmar cyclone, earthquakes in China), US-CERT would like to remind users to remain cautious when receiving unsolicited email requests for donations from charitable organizations. These unsolicited requests could be potential phishing scams.

These phishing incidents underscore the importance of maintaining up-to-date patches and anti-virus signatures, along with recognizing social engineering tactics. To educate users about social engineering, phishing attacks, and handling malicious attachments, review US-CERT Cyber Security Tips "*Avoiding Social Engineering and Phishing Attacks*" and "*Using Caution with Email Attachments*."

# Exploitation of Adobe Flash Player Vulnerability

In May 2008, US-CERT received reports of active exploitation of a vulnerability affecting Adobe Flash Player. The vulnerability may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system and can be exploited via a specially crafted Flash file (e.g., SWF) that may be hosted or embedded in a web page. If an attacker gains control of a website or web server, this vulnerability may also be exploited by trusted sites. Reports indicated that this vulnerability was being actively exploited in conjunction with the recent SQL injection and cross-site scripting attacks, which affected thousands of web pages.

US-CERT released Vulnerability Note VU#159523 "Adobe Flash Player Integer Overflow Vulnerability" and Technical Cyber Security Alert TA08-149A "Exploitation of Adobe Flash Vulnerability" to provide more details and mitigation strategies to protect against this vulnerability.

[1] http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9094198
[2] http://www.uscourts.gov/newsroom/2008/alert.cfm

## SNMPv3 Authentication Bypass Vulnerability

Net-SNMP released a patch to address a vulnerability affecting implementations of SNMPv3 (CVE-2008-0960). The Simple Network Management Protocol (SNMP) is a widely deployed protocol that is commonly used to monitor and manage network devices. The vulnerability exists in the way implementations of SNMPv3 handle specially crafted packets and may allow authentication bypass. Attackers exploiting this vulnerability can view and/or modify the configuration of these devices. Note that the attacker must authenticate as a user with write privileges in order to modify the configuration of the affected device.

US-CERT released Vulnerability Note VU#878044 to provide details and mitigation strategies.

## National Cyber Alert System

Stay informed and involved by subscribing to the products included in the US-CERT National Cyber Alert System. There are five products available for various technical levels and needs. They are as follows:

**Current Activity** – Notifies users of the most frequent, high-impact types of security incidents currently reported to US-CERT.

**Technical Cyber Security Alerts** – Provide timely information about current security issues, vulnerabilities, and exploits.

**Cyber Security Bulletins** – Summarize information that has been published about new vulnerabilities.

**Cyber Security Alerts** – Alert non-technical readers to security issues that affect the general public.

**Cyber Security Tips** – Provide information and advice for non-technical readers about a variety of common security topics.

Visit http://www.us-cert.gov/cas/signup.html to learn more

## Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, provide a tip of suspicious activity, or just learn more about cyber security, please use one of the below methods.

If you would like to provide feedback on this report, or if you have comments or suggestions for future reports, please email info@us-cert.gov.

| | |
|---|---|
| Web Site Address: | http://www.us-cert.gov |
| Email Address: | info@us-cert.gov |
| Phone Number: | +1 (888) 282-0870 |
| PGP Key ID: | 0x17B1C7F7 |
| PGP Key Fingerprint: | 3219 08A0 716E 50DA 3ECF 501D 6780 28A0 17B1 C7F7 |

PGP Key: https://www.us-cert.gov/pgp/info.asc

## Disclaimer

The purpose of the analysis within this report is to provide awareness and information on cyber threats as seen and reported to US-CERT. The content of this report was developed with the best information available at the time of analysis; if further information becomes available, US-CERT may publish it in a future report.