



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary - August 2012 -

This report summarizes general activity including updates to the [National Cyber Awareness System](#) in August 2012. It includes current activity updates, alerts, and bulletins, in addition to other newsworthy events or highlights.

Executive Summary

During August 2012, US-CERT issued three Current Activity entries, two Alerts, and four weekly Bulletins.

Highlights for this month include updates or advisories released by Microsoft and Oracle.

Contents

Executive Summary	1
Current Activity	1
Alerts	2
Bulletins	2
Security Highlights	2
Contacting US-CERT	2

Current Activity

[Current Activity](#) entries are high-impact security threats and vulnerabilities currently reported to US-CERT. The table lists all of the entries posted this month followed by a brief overview of the most significant entries.

Current Activity for August 2012	
August 15	Microsoft Releases August Security Bulletin
August 28	US-CERT Releases Oracle Java JRE 1.7 Security Advisory
August 28	Malware Campaigns Impersonating U.S. Government Agencies

- Microsoft released updates to address vulnerabilities in Microsoft Windows, Internet Explorer, Office, SQL Server, Server Software, Developer Tools, and Exchange Server as part of the Microsoft Security Bulletin Summary for [August 2012](#). These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or operate with elevated privileges. US-CERT encourages users and administrators to review the bulletin and follow best-practice security policies to determine which updates should be applied. Additional information regarding the bulletin can be found in US-CERT Technical Alert [TA12-227A](#).
- US-CERT released Vulnerability Note [VU#636312](#) to address a vulnerability in Oracle Java Runtime Environment (JRE) 1.7. This vulnerability may allow an attacker to execute arbitrary code on a vulnerable system. Oracle released an out-of-band patch to address this vulnerability. US-CERT encourages users and administrators to review the [Oracle Security Alert for CVE-2012-4681](#) and apply any necessary updates to help mitigate the risk.

Alerts

[Alerts](#) provide timely information about current security issues, vulnerabilities, and exploits.

<i>Alerts for August 2012</i>	
<i>August 14</i>	TA12-227A Microsoft Updates for Multiple Vulnerabilities
<i>August 27</i>	TA12-240A Oracle Java 7 Security Manager Bypass Vulnerability

Bulletins

[Bulletins](#) are issued weekly and provide a summary of new vulnerabilities recorded by the National Institute of Standards and Technology's (NIST's) [National Vulnerability Database \(NVD\)](#). The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSA)/US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

<i>Bulletins for August 2012</i>	
<i>August 6</i>	SB12-219 Vulnerability Summary for the Week of July 30, 2012
<i>August 13</i>	SB12-226 Vulnerability Summary for the Week of August 6, 2012
<i>August 20</i>	SB12-233 Vulnerability Summary for the Week of August 13, 2012
<i>August 27</i>	SB12-240 Vulnerability Summary for the Week of August 20, 2012

A total of 703 vulnerabilities were recorded in the NVD during August 2012.

Security Highlights

Malware Campaigns Impersonating U.S. Government Agencies

US-CERT is aware of multiple malware campaigns impersonating multiple U.S. Government agencies, including the United States Cyber Command (USCYBERCOM) and the Federal Bureau of Investigation (FBI). Once installed on a system, the malware displays a screen claiming that a Federal Government agency has identified the user's computer as being associated with one or more crimes. The user is told to pay a fine to regain the use of the computer, usually through prepaid money card services. Affected users should not follow the payment instructions. US-CERT encourages users to follow the recommendations in Security Tip ST05-006, Recovering from Viruses, Worms, and Trojan Horses. Users may also choose to file a complaint with the FBI's Internet Crime Complaint Center (IC3).

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or learn more about cybersecurity, please use one of the methods listed below. 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.

Website Address: <http://www.us-cert.gov>

Email Address: soc@us-cert.gov

Phone Number: +1 888-282-0870

PGP/GPG Key: [0x91D70D64](#)

PGP Key Fingerprint: F68D 07E5 FC48 403F C989 AC73 2A4C 5804 0FA6 ED7D

PGP Key: <https://www.us-cert.gov/pgp/soc.asc>