US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- October 2011 -

This report summarizes general activity including updates to the National Cyber Alert System in October 2011. It includes current activity updates, technical and non-technical cyber security alerts, and cyber security bulletins, in addition to other newsworthy events or highlights.

Executive Summary

During October 2011, US-CERT issued 13 Current Activity entries, 2 Technical Cyber Security Alerts, 2 Cyber Security Alerts, and 5 weekly Cyber Security Bulletins.

Highlights for this month include updates or advisories released by Microsoft, Apple, Google, Apache, Oracle, and Cisco.

Contents

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 October 2011	
October 4	Google Releases Chrome 14.0.835.202
October 5	Cisco Releases Multiple Security Advisories
October 6	Microsoft Releases Advance Notification for October Security Bulletin
October 7	Apache HTTP Server Reverse Proxy Bypass
October 11	Microsoft Releases October Security Bulletin
October 11	Apple Releases iTunes 10.5
October 12	Apple Releases Multiple Security Updates
October 17	Oracle Pre-Release Announcements for October 2011
October 18	Oracle Releases Critical Patch Update for October 2011
October 19	Cisco Releases Two Security Advisories
October 25	Google Releases Chrome 15.0.874.102
October 26	Cisco Releases Multiple Security Advisories
October 27	Apple Releases QuickTime 7.7.1

- Microsoft released Security Bulletin MS11-077 to address vulnerabilities in Microsoft Windows, Internet Explorer, .NET Framework, Silverlight, Forefront United Access Gateway, and Microsoft Host Integration Server as part of the Microsoft Security Bulletin Summary for October 2011. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or operate with elevated privileges. Please see US-CERT Vulnerability Note VU#619281 for additional information regarding the most severe vulnerability identified in the Microsoft Security Bulletin.
- Apple released multiple security updates during the month of October 2011:
    - iTunes 10.5 addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
    - Security updates for Apple iOS, Safari 5.1.1, OS X Lion v10.7.2, iWork 09, and Apple TV 4.4 address multiple vulnerabilities; exploitation of these vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, obtain sensitive information, and bypass security restrictions.
    - QuickTime 7.7.1 addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or obtain sensitive information.
- Google released two updates to its Chrome web browser, Chrome 14.0.835.202 and Chrome 15.0.874.102 for Linux, Mac, Windows, and Chrome Frame to address multiple vulnerabilities that may allow an attacker to execute arbitrary code.
- The Apache Foundation issued a Security Advisory addressing a vulnerability in Apache HTTP Server's reverse proxy mode. Successful exploitation of this vulnerability may allow a remote attacker to gain access to internal systems.
- Oracle released its Critical Patch Update and Java SE Critical Patch Update Advisory for October 2011 to address 77 vulnerabilities across multiple products, including Oracle Database Server, Oracle Fusion Middleware, Oracle E-Business Suite, Oracle Supply Chain Products Suite, Oracle PeopleSoft Products, Oracle Siebel CRM, Oracle Industry Applications, Oracle Sun Products Suite, Oracle Linux, Oracle Virtualization, and Oracle Java SE.
- Cisco released multiple security advisories throughout the month of October:
    - Cisco released security advisories to address vulnerabilities affecting Cisco ASA 5500 Series Adaptive Security Appliances, Cisco Catalyst 6500 Series ASA Services Module, Cisco Firewall Services Module, Cisco Network Admission Control Manager, Cisco Unified Contact Center, Cisco WebEx Player, Cisco Security Agent, and Cisco Unified Communication Manager. These vulnerabilities may allow an attacker to cause a denial-of-service condition, bypass authentication mechanisms, or obtain sensitive information.
    - Cisco released security advisories to address vulnerabilities affecting CiscoWorks Common Services and Cisco Show and Share that may allow an attacker to execute arbitrary code or bypass security restrictions.

Technical Cyber Security Alerts

Technical Cyber Security Alerts provide timely information about current security issues, vulnerabilities, and exploits.

Technical Cyber Security Alerts for October 2011	
October 11	TA11-284A Microsoft Updates for Multiple Vulnerabilities
October 13	TA11-286A Apple Updates for Multiple Vulnerabilities

Cyber Security Alerts

Cyber Security Alerts provide timely information about current security issues, vulnerabilities, and exploits. They outline the steps and actions that non-technical home and corporate users can take to protect themselves.

Cyber Security Alerts (non-technical) for October 2011	
October 11	SA11-284A Microsoft Updates for Multiple Vulnerabilities
October 13	SA11-286A Apple Updates for Multiple Vulnerabilities

Cyber Security Bulletins

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

Cyber Security Bulletins for October 2011	
October 3	SB11-276 Vulnerability Summary for the Week of September 26, 2011
October 10	SB11-283 Vulnerability Summary for the Week of October 3, 2011
October 18	SB11-290 Vulnerability Summary for the Week of October 10, 2011
October 24	SB11-297 Vulnerability Summary for the Week of October 17, 2011
October 31	SB11-304 Vulnerability Summary for the Week of October 24, 2011

A total of 484 vulnerabilities were recorded in the NVD during October 2011.

Security Highlights

Microsoft Releases Advance Notification for October Security Bulletin

Microsoft has issued a Security Bulletin Advance Notification indicating that its October release will contain eight bulletins. These bulletins will have the severity ratings of critical and important and will be for Microsoft .NET Framework, Microsoft Silverlight, Microsoft Windows, Internet Explorer, Microsoft Forefront Unified Access Gateway, and Microsoft Host Integration Server. Release of these bulletins is scheduled for Tuesday, October 12, 2011.

US-CERT will provide additional information as it becomes available.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or learn more about cyber security, 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 e-mail info@us-cert.gov.

Web Site Address: http://www.us-cert.gov
E-mail Address: info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: 0xEDA10949
PGP Key Fingerprint: 6040 50FC 1BA3 81FA 0919 1378 C036 EDA1 0949
PGP Key: https://www.us-cert.gov/pgp/info.asc