Customer Service and Support
Security

MICROSOFT SECURITY BULLETIN ALERT

CONFIDENTIALITY RATING: PARTNER LEVEL NDA EXCEPT FOR CUSTOMER-READY EMAILS ATTACHED.

What is the purpose of this alert?

This alert is to provide you with an overview of the new security bulletin being released (out-of-band) on December 29, 2011.

New Security Bulletin

Microsoft is releasing one new security bulletin (out-of-band) for newly discovered vulnerabilities:

Bulletin ID	Bulletin Title	Maximum Severity Rating	Vulnerability Impact	Restart Requirement	Affected Software*
MS11-100	Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)	Critical	Elevation of Privilege	This update may require a restart	All supported versions of ASP.NET on all supported versions of Windows and Windows
* Where indicated in the Affected Software table on the bulletin webpage, the vulnerabilities addressed by this update may affect supported editions of Windows Server 2008 or Windows Server 2008 R2, when installed using the Server Core installation option. Affected software listed above is an abstract. Please see the security bulletin at the link provided for complete details.					

PUBLIC BULLETIN WEBCAST
Microsoft will host a webcast to address customer questions on this bulletin:

Title: Information About Microsoft's December 2011 Out-of-Band Security Bulletin Release
Date: Thursday, December 29, 2011, at 1:00 P.M. (GMT-08:00) Pacific Time (U.S. & Canada)
URL: https://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032502798

PUBLIC RESOURCES RELATED TO THIS ALERT
Security Bulletin MS11-100 – Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420): http://technet.microsoft.com/security/bulletin/MS11-100

Security Advisory 2659883 – Vulnerability in ASP.NET Could Allow Denial of Service http://technet.microsoft.com/security/advisory/2659883

Microsoft Security Response Center (MSRC) Blog: http://blogs.technet.com/msrc/

Microsoft Security Research & Defense (SRD) Blog: http://blogs.technet.com/srd/

CSS Security (Internal) Blog: http://securityblog/

ACTIONS REQUIRED - SERVICES

Premier: This is a Level 3 Alert, requiring the broadest outreach. Please review and understand this information. Plan to attend the CSS Security conference call if you need additional details on the alerts for your customers. You must take the following actions:

Send the attached Premier customer-ready email as soon as possible. **NOTE:** You must include your virtual account team in the **Cc** line on this communication. To protect PII, please use the **Bcc** field when sending email to multiple customers in the same message.

Call your customers within 24 hours, including outside of normal business days or hours.

MCS: Read the internal-only field bulletin located at http://bulletinportal/ to understand this issue and be prepared to respond to customer questions reactively. The Account Manager will coordinate contact with your customers' Emergency Response Lead. Please support your Account Manager as needed.

CSS: Customers may be calling in about this issue. Please review the preceding information, and be prepared to assist our customers in dealing with the application of this update and its impact on their environment. Please feel free to use the customer-ready email message. To protect PII, please use the **Bcc** field when sending email to customers.

Customer Service: Please review the preceding information, and route customer inquiries in relation to this bulletin as per local Security Incident Handling procedures. Local management teams will send notifications if Emergency Response Plans and routing procedures have been initiated.

Contacts: For technical questions please contact queue 82212 or our external direct dial (888) HELPSEC line at (888) 435-7732. This line is open 24x7 and can be dialed from all international locations (although it is a toll call from outside the U.S. and Canada). **NOTE:** This is for Microsoft personnel and partners only. Do not give this number to customers directly.

All: The actions required for field communication at each alert level are defined by the Security Response Matrix: http://sharepoint/sites/bulletinportal/Alerts/Pages/ResponseMatrix.aspx.

ACTIONS REQUIRED – SALES / EPG

Enterprise Account Managers should read the internal-only field bulletin located at http://bulletinportal/ to understand this issue and be prepared to respond to customer questions. If your customer is Premier, contact the TAM/ADC to confirm they have initiated communication, and then coordinate the active account team to call the Emergency Response Lead as listed in Siebel. If your customer is not Premier, coordinate with the active account team to call the Emergency Response Lead as listed in Siebel.

Enterprise Account TSs should read the internal-only field bulletin located at http://bulletinportal/ to understand this issue. The Account Manager will coordinate contact with your customers' Emergency Response Lead. Please support your Account Manager as needed.

Partner Account Managers should read the internal-only field bulletin located at http://bulletinportal/ to understand this issue. Use the attached Product Support Services customer-ready email message to proactively communicate with your Partner.

All: The actions required for field communication at each alert level are defined by the Security Response Matrix: http://sharepoint/sites/bulletinportal/Alerts/Pages/ResponseMatrix.aspx.

ACTIONS REQUIRED – SALES & MARKETING / SMS&P

Mid-Market Managers should make this internal-only field bulletin located at http://bulletinportal/ available to telesales managers to ensure they understand this issue, are prepared to answer customer questions reactively, and can direct customers to guidelines for securing their PCs at http://www.microsoft.com/security/.

U.S. Telesales Leads should read the internal-only field bulletin located at http://bulletinportal/ to ensure you understand this issue, are prepared to answer customer questions reactively, and can direct customers to guidelines for securing their PCs at http://www.microsoft.com/security/.

Small Business Marketing Teams should continue to direct Small Business customers to http://www.microsoft.com/security to download security updates and access all security updates and information.

Partner Account Managers (PAMs/PEMs) should review the content in this alert to understand associated issues and be prepared to respond to customer questions reactively. Additional details associated with security bulletin and advisory releases are published on the CSS Security bulletin portal http://bulletinportal/. All partner field personnel should know where to go for all security related updates and information and be prepared to provide information to partners. The most up-to-date security information and security updates can be found at http://technet.microsoft.com/security.

Partners subscribing to our Security Notification Service and/or Security Update Service will receive this information via email. Breadth partners should be directed to http://technet.microsoft.com/security for the most current information on this and all security alerts and encouraged to sign up for automatic security alerts to ensure they receive timely notification.

All: The actions required for field communication at each alert level are defined by the Security Response Matrix: http://sharepoint/sites/bulletinportal/Alerts/Pages/ResponseMatrix.aspx.

INTERNAL RESOURCES RELATED TO THIS ALERT

CSS Security Bulletin Information Portal provides bulletin slide decks, FAQs, support trends, and analysis at http://bulletinportal/.

CSS Security Blog also provides late-breaking bulletin support information at http://securityblog/.

EXTERNAL COMMUNICATION RELATED TO THIS ALERT

Security Notification Service (Basic): An email regarding new security bulletins is sent to IT professionals who have subscribed to receive this notification.

Security Notification Service (Comprehensive): An email regarding new security bulletins is sent to IT professionals who have subscribed to receive this notification.

NEW SECURITY BULLETIN TECHNICAL DETAILS

In the following table of affected software, software editions that are not listed are past their support lifecycle. To determine the support lifecycle for your product and edition, visit the Microsoft Support Lifecycle website at http://support.microsoft.com/lifecycle/.

Bulletin Identifier	Microsoft Security Bulletin MS11-100
Bulletin Title	**Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)**
Executive Summary	This security update resolves one publicly disclosed vulnerability and three privately reported vulnerabilities in Microsoft .NET Framework. The most severe of these vulnerabilities could allow elevation of privilege if an unauthenticated attacker sends a specially crafted web request to the target site. An attacker who successfully exploited this vulnerability could take any action in the context of an existing account on the ASP.NET site, including executing arbitrary commands. The security update addresses the vulnerabilities by correcting the manner in which the .NET Framework handles specially crafted requests, and the manner in which the ASP.NET Framework authenticates users and handles cached content. This security update also addresses the vulnerability first described in Microsoft Security Advisory 2659883.
Affected Software	This security update is rated Critical for Microsoft .NET Framework 1.1 Service Pack 1, Microsoft .NET Framework 2.0 Service Pack 2, Microsoft .NET Framework 3.5 Service Pack 1, Microsoft .NET Framework 3.5.1, and Microsoft .NET Framework 4 on all supported editions of Microsoft Windows.
CVE, Exploitability Index Rating	CVE-2011-3414: Collisions in Hash Table May Cause DoS Vulnerability (EI = 3) CVE-2011-3415: Insecure Redirect in .NET Forms Authentication Vulnerability (EI = NA) CVE-2011-3416: ASP.NET Forms Authentication Bypass Vulnerability (EI = 1) CVE-2011-3417: ASP.NET Forms Authentication Ticket Caching Vulnerability (EI = 2)
Attack Vectors	An unauthenticated attacker could send a small number of specially crafted ASP.NET requests to an affected ASP.NET site, causing a denial of service condition. (CVE-2011-3414) An attacker could create a specially crafted URL and convince a user to click it. After the user logs on to an expected website, the attacker then redirects the user to a website controlled by the attacker. Once there, the attacker could convince the user to divulge information otherwise intended to remain private. (CVE-2011-3415) An unauthenticated attacker would need to obtain a valid account name to the site. The attacker could then craft a special web request using a previously registered account name to gain access to that account. (CVE-2011-3416) An attacker could exploit the vulnerability by sending a specially crafted link to the user and convincing the user to click the link. (CVE-2011-3417)

Mitigating Factors

CVE-2011-3414 (Collisions in Hash Tables May Cause DoS Vulnerability)

- By default, IIS is not enabled on any Windows operating system.
- Sites that disallow “application/x-www-form-urlencoded” or “multipart/form-data” HTTP content types are not vulnerable.

CVE-2011-3415 (for Insecure Redirect in .NET Form Authentication Vulnerability)

- This vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to produce information that could be used to try to further compromise user information.
- By default, installing ASP.NET does not enable Forms Authentication. It has to be explicitly configured per-application to be enabled.
- IIS is not installed by default.
- By default, ASP.NET is not installed when .NET Framework is installed. Only customers who manually install and enable ASP.NET are likely to be vulnerable to this issue.
- The attacker would have to convince the user to click a link in order to exploit the vulnerability.

CVE-2011-3416 (Forms Authentication Bypass Vulnerability)

- An attacker must be able to register an account on the ASP.NET application, and must know an existing user name.
- By default, installing ASP.NET does not enable Forms Authentication. It has to be explicitly configured per-application to be enabled.
- IIS is not installed by default.
- By default, ASP.NET is not installed when .NET is installed. Only customers who manually install and enable ASP.NET are likely to be vulnerable to this issue.

CVE-2011-3417 (Forms Authentication Ticket Caching Vulnerability)

- By default, ASP.NET responses are not cached by the OutputCache. The developer of the site has to opt-in to output caching via the OutputCache directive on a page.
- An attacker who successfully exploited this vulnerability could gain the same user rights as the target user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.
- By default, IIS is not installed on any affected operating system version. Only customers who manually install this are likely to be vulnerable to this issue.
- By default, ASP.NET is not installed when .NET is installed. Only customers who manually install and enable ASP.NET are likely to be vulnerable to this issue.

REGARDING INFORMATION CONSISTENCY

We strive to provide you with accurate information in static (this mail) and dynamic (web-based) content. Microsoft's security content posted to the web is occasionally updated to reflect late-breaking information. If this results in an inconsistency between the information here and the information in Microsoft's web-based security content, the information in Microsoft's web-based security content is authoritative.

DISTRIBUTION

Bcc:

Level 0 Audience	PREMALL; SMESEC; CSSSECE; SCONALL; SPIMAIL; FLSSIRP; USESFTEA; CSCPEFT; CPE13FTE; SECWW; NOTIFYME
Level 1 and 2 Additions	USNST; WWSECCOM; USFSSIRP