|  |
| --- |
|  |
| |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  | | --- | |  | | Trustworthy Computing | June 2014 | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_MS_logo.jpg | | Microsoft Security Newsletter |  | |  |  | |  | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  | | --- | |  | | Welcome to June’s Security Newsletter! | | Last month, we covered the top threats facing enterprise organizations and how to help protect against them. This month’s newsletter focuses on security guidance for data protection and, specifically, public key infrastructure (PKI), which many organizations have in place to support data protection and authentication.   If attackers successfully gain access to your organization’s PKI, this can expose your organization to serious risk. To help you design PKIs and protect this infrastructure from emerging threats, Microsoft IT, Microsoft’s IT department, has released a detailed technical reference document entitled “[Securing Public Key Infrastructure](http://click.email.microsoftemail.com/?qs=8fdab5af173b5ad261dd16a61ceddb2d7c2490cf937fc08f5b0a8db22ecdbc20119b5a2fe74d6549).” Included in the document you will find guidance on:   |  |  | | --- | --- | | • | Common vectors for PKI compromise | | • | Planning cryptographic algorithms and certificate usages | | • | Designing physical security | | • | Implementing technical controls to secure PKI | | • | Protecting PKI artifacts and assets | | • | Monitoring PKI for malicious activity | | • | Recovering from a compromise |   If you are an IT professional and have a PKI running in your environment, I encourage you to download and read the paper—and consult the resources listed below for additional guidance. I hope you find these resources helpful.   |  |  |  | | --- | --- | --- | | Tim Rains |  | Best regards, Tim Rains, Director Microsoft Trustworthy Computing |   Have feedback on how we can improve this newsletter? Email us at [secnlfb@microsoft.com](mailto:secnlfb@microsoft.com) and share your ideas. | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | | |  |  |  | | --- | --- | --- | | Top Stories | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_top.jpg](#top) | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_next.jpg](#SecurityGuidance) | | |  | | [Who Exploits Vulnerabilities: the Path from Disclosure to Mass Market Exploitation](http://click.email.microsoftemail.com/?qs=8fdab5af173b5ad23c5254dda49168aa8d92a2dfeb43b5953da96e1878195c7036c5efc421b83798)  Vulnerabilities are weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of the software or the data that it processes. Learn why the parties that initially disclose vulnerabilities are not always the same parties that go on to develop and use exploits that take advantage of them—and what you can do to mitigate the risk rom exploits.   [When Vulnerabilities are Exploited: the Timing of First Known Exploits for Remote Code Execution Vulnerabilities](http://click.email.microsoftemail.com/?qs=8fdab5af173b5ad28c5b959cb5bbfc1f01d2dda2229dad2dddf80622f2ea96aedaedb699ea24a521)  Every wonder how many days of risk exist between the time that a vulnerability is disclosed and when we first see active exploitation of it; i.e. how long do organizations have to deploy the update before active attacks are going to happen? Explore the Trustworthy Computing Security Science team’s new data from the recently released [Microsoft Security Intelligence Report volume 16](http://click.email.microsoftemail.com/?qs=8fdab5af173b5ad2c7b88e6e3bda4e624ed54894d0a9ac21b84c7a8ff2a679dc242b9b661eb3c514).   [Keeping Oracle Java Updated Continues to be High Security ROI](http://click.email.microsoftemail.com/?qs=8fdab5af173b5ad2ccf15818f9053acfa58f86796ec0e84512ab2731af10f9592b16553e32260276)  One of the most popular tactics attackers use to try to exploit vulnerabilities in Java is using exploit kits. Learn why keeping Java up-to-date with security updates is one of the most effective ways to protect environments from attackers. | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | | |  |  |  | | --- | --- | --- | | Security Guidance | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_top.jpg](#top) | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_next.jpg](#CloudSecurityCorner) | | | [Security Tip of the Month: Enterprise PKI with Windows Server 2012 R2 Active Directory Certificate Services](http://click.email.microsoftemail.com/?qs=8fdab5af173b5ad279ce1151b6b5c2dcc78773aafca38843a26f61f4da1255d9b1960cac723f1ad5)  PKI is heavily employed in cloud computing for encrypting data and securing transactions. While Windows Server 2012 R2 is developed as a building block for cloud solutions, there is an increasing demand for IT professionals to acquire proficiency on implementing PKI with Windows Server 2012 R2. This two-part blog post series ([click here for Part 2](http://click.email.microsoftemail.com/?qs=8fdab5af173b5ad2717bcaf3b2f34f86b88d3635f8862fb2de7000cae7aae768da759c3afa18881c)) will help you implement a simple PKI for assessing or piloting solutions, and better understand and become familiar with the process.   [Best Practices for Securing Active Directory](http://click.email.microsoftemail.com/?qs=8fdab5af173b5ad22b782c304c66386ffd231528553ccf9390f89975da7394d9c6e3e87aad368ff9)  Download recommendations to enhance the security of Active Directory installations. Learn about common attacks against Active Directory, the countermeasures you can take to reduce the attack surface, and get recommendations for recovery.   [Trusted Platform Module (TPM) Fundamentals](http://click.email.microsoftemail.com/?qs=8fdab5af173b5ad2acb17fd6cf8f218e08e62fd59c78dabab36b4a57de95d6839b0390b6b6b52b7d)  Explore the components of the [Trusted Platform Module](http://click.email.microsoftemail.com/?qs=8fdab5af173b5ad2adaae0ee0b550907a4aac00d6ee8ebd426333a022e53b3265a30df4f09533306) (TPM 1.2 and TPM 2.0) and learn how they are used to mitigate dictionary attacks. Looking for more TPM guidance? Check out these resources:   |  |  | | --- | --- | | • | [Initialize and Configure Ownership of the TPM](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3bbd4e7c490c8af352bdfb62c9458c64faf9a00a69e686d406a3a2eb574e5ccb0) | | • | [TPM Services Group Policy Settings](http://click.email.microsoftemail.com/?qs=9368efa76acefbc31d42b7c6f87b3a72611dfbbdc875379638ceac5520f54f33be4e5eb9046693a4) | | • | [Backup the TPM Recovery Information to Active Directory Domain Services (AD DS)](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3ea428a9f09ee9bd3b693daf446b2bd337ede6e6a35200095fa91c6c027c41941) | | • | [Manage TPM Commands](http://click.email.microsoftemail.com/?qs=9368efa76acefbc38ed6f2a7cbf48aa2c52dff8f57d00c1f454f29deb7b53936d552d128ff3049c6) | | • | [Manage TPM Lockout](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3890699441725081fc54b3afd29655b45706d1d1d29d667e10cbd5b6482e2f08a) |   [TPM Platform Crypto-Provider Toolkit](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3122c469dc4369a6b6f264cb4bc70a9575f2d366ae51460ee69d42eade8a405fe)  Download sample code, utilities and documentation for using TPM-related functionality in Windows 8. Subsystems described include the TPM-backed Crypto-Next-Gen (CNG) platform crypto-provider, and how attestation-service providers can use the new Windows features. Both TPM1.2 and TPM2.0-based systems are supported.   [PKI Certificate Requirements for Configuration Manager](http://click.email.microsoftemail.com/?qs=9368efa76acefbc368987d9e889e3a7f6d437511601997459e2b62ed74be86a9d8b6f811b4c99cfd)  Find a list of the PKI certificates you might require for System Center 2012 Configuration Manager. This information assumes basic knowledge of PKI certificates. For step-by-step guidance and for an example deployment of these certificates, see [Step-by-Step Example Deployment of the PKI Certificates for Configuration Manager: Windows Server 2008 Certification Authority](http://click.email.microsoftemail.com/?qs=9368efa76acefbc39af1e84e17ccf15938f9701ad0cbeaeeae2d63add531e8636516fa5761371040). | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | | |  |  |  | | --- | --- | --- | | Community Update | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_top.jpg](#top) | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_next.jpg](#CloudSecurityCorner) | | | [Public Key Infrastructure Design Guidance](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3395c83a2a625418cde2d19c168bf0f1f843a029bd0416fabe3eb056c6f31cf3f)  Before you configure a PKI and certification authority (CA) hierarchy, you should be aware of your organizations security policy and certificate practice statement (CPS). Explore your design options and find links to examples of policy statements if your organization does not currently have one.   [Active Directory Certificate Services (AD CS) PKI Design Guide](http://click.email.microsoftemail.com/?qs=9368efa76acefbc351d28cb9e9e7d845a98edff0d8d98705bd52b6c454ea6963e66790efccc24128)  While Windows Server 2012 products provides a variety of secure applications and business scenarios based on the use of digital certificates, you need to design a public key infrastructure (PKI) before you can use those certificates. Check out this step-by-step wiki guide for guidance on everything from identifying your AD CS deployment goals to creating a certificate management plan. | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | | |  |  |  | | --- | --- | --- | | This Month's Security Bulletins | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_top.jpg](#top) | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_next.jpg](#EventsAndTraining) | | |  | | June 2014 Security Bulletins   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Critical   |  | | --- | |  | | • | MS14-035: | 2969262 | [Cumulative Security Update for Internet Explorer](http://click.email.microsoftemail.com/?qs=9368efa76acefbc335c6a84f41d29dfca5e1fa1d8941274d6e7c15a9836c7871be432af138f42f36) | |  | | | | | • | MS14-036: | 2967487 | [Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3a6b882724188d3918c9229a3b04b2f5ac5b4afa71fc921788680d6f105554c07) |   Important   |  | | --- | |  | | • | MS14-034: | 2969261 | [Vulnerability in Microsoft Word Could Allow Remote Code Execution](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3b94831af674196c1fc0b8a590880d80187d8178453b4847649e99024d1ba2bd9) | |  | | | | | • | MS14-033: | 2966061 | [Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure](http://click.email.microsoftemail.com/?qs=9368efa76acefbc30353c45e7a5c6f1d866dd3157a842e8726342e1c0498295a24fb52231df3b039) | |  | | | | | • | MS14-032: | 2969258 | [Vulnerability in Microsoft Lync Server Could Allow Information Disclosure](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3caa2eb211ed391e0267232151a0faa122f560d1dacf4a650c83f424024287b65) | |  | | | | | • | MS14-031: | 2962478 | [Vulnerability in TCP Protocol Could Allow Denial of Service](http://click.email.microsoftemail.com/?qs=9368efa76acefbc38aad218d3980435bce9bf09a5d649764d4de35392b5caa52759e0235baa39eaa) | |  | | | | | • | MS14-030: | 2969259 | [Vulnerability in Remote Desktop Could Allow Tampering](http://click.email.microsoftemail.com/?qs=9368efa76acefbc314a1427e595301adfa561390faffa5960c1bf3ed61609847288f190a7f283e3d) | | | |  | | June 2014 Security Bulletin Resources:   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | • | [Theoretical Thinking and the June 2014 Bulletin Release](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3ba535c7cce9ebe59f8b388bcbcf5f3736ddc7eebac5942f17c63fd0bee67b906) | | • | [June 2014 Security Bulletin Webcast](http://click.email.microsoftemail.com/?qs=9368efa76acefbc304a76c68c51db22cc93edc22feb43fabdbd8ad735a7f8060b210898291b80c2f) | | • | [June 2014 Security Bulletin Webcast Q&A](http://click.email.microsoftemail.com/?qs=9368efa76acefbc33f15a1b1f9b1940d4b3d3f6b412828273babceda275b4711d363aa9263d5cdb8) | | • | [Malicious Software Removal Tool: June 2014 Update](http://click.email.microsoftemail.com/?qs=9368efa76acefbc35b3c6513aa160868c15af58cd0ff22244834612f7c7f4119da484ca2f70c40d9) | | | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | | |  |  |  | | --- | --- | --- | | Security Events and Training | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_top.jpg](#top) | [http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_next.jpg](#resources) | | |  | | [Defense in Depth: Windows 8.1 Security](http://click.email.microsoftemail.com/?qs=9368efa76acefbc307e6de5691cc92be7e2d1cd6ba16087fc8cf684c57dd37c9debb9df8bdcc3f8b)  See how Windows 8.1 addresses security as a whole system, one layer at a time with this seven-module course from Microsoft Virtual Academy. Explore methods of developing a secure baseline and learn how to harden your Windows enterprise architectures from pass-the-hash and other advanced attacks.   [Office 365 Education Technical Overview](http://click.email.microsoftemail.com/?qs=9368efa76acefbc39ac97bd35e80020c1b153fae4e98f9689f797c554c79cb72176b6b2969339259)  Wednesday, July 16, 2014 – 1:00PM Central Time Better understand the technical tools and resources of Office 365 Education, and learn how to support the unique needs of your school without sacrificing identity management and other security and compliance measures. This session will also be conducted every Wednesday at this time in August.   [Office 365 Education Deployment Overview](http://click.email.microsoftemail.com/?qs=9368efa76acefbc31ef0a483a070d278b19606280f62d6924b44e7437cab9cc21a9e79621587a9d9)  Thursday, July 24, 2014 – 1:00PM Central Time Compare your Microsoft Office 365 for education deployment options and learn about the terminology and tools available to streamline your deployment. Topics will include networking, identity management, hybrid deployments, and synchronization. This session will also be conducted every Wednesday at this time in August. | |  | | http://image.email.microsoftemail.com/lib/fe68157075670478701d/m/1/51148_Security_Newsletter_2013_borderLine.jpg | |  | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Essential Tools   |  |  | | --- | --- | |  | | | • | [Microsoft Security Bulletins](http://click.email.microsoftemail.com/?qs=9368efa76acefbc37a5aee07b00c2b9ead20998eb5465e37c9fc7213a2ca754e0f1cfaa7499c6c90) | |  | | | • | [Microsoft Security Advisories](http://click.email.microsoftemail.com/?qs=9368efa76acefbc396c493348de51273a308f9499af39dad43306872cb4dd2153b9378563d2b533c) | |  | | | • | [Security Compliance Manager](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3456fa0558b855a238996f08f84c478d40981101645ffeca4f22832190fce48c2) | |  | | | • | [Microsoft Security Development Lifecycle Starter Kit](http://click.email.microsoftemail.com/?qs=9368efa76acefbc389e47d27b31f1239581e73b7f2c83eea20fdbc79e2564cb33c176fb245d68c9b) | |  | | | • | [Enhanced Mitigation Experience Toolkit](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3ac54b943be3c07a96c27125a68bad97f6f90ba5e737294db3569a9feadc21ba1) | |  | | | • | [Malicious Software Removal Tool](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3d85ca9d72e23ab1a7f2da052316c39e13ec0e814fa3f7fbb9064e8c862d45031) | |  | | | • | [Microsoft Baseline Security Analyzer](http://click.email.microsoftemail.com/?qs=9368efa76acefbc33554a13abbb12c07b9f8dac792bea17df47b267b34bc0dc85e7ed732dc5ef153) | | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Security Centers   |  |  | | --- | --- | |  | | | • | [Security TechCenter](http://click.email.microsoftemail.com/?qs=9368efa76acefbc312fb196d2d7e007aecf7c6cf678ec02a243917ff160c338ba5596fc9d39f4565) | |  | | | • | [Security Developer Center](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3cbe9df44da4764917b96ae328cf6d0ed223f4c5c7844bf3cef2af0783a2ac3a2) | |  | | | • | [Microsoft Security Response Center](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3e4dfda40e48b3af2cf118b18cc1ead6cbfb0a96b213d856742496f6169b85b33) | |  | | | • | [Microsoft Malware Protection Center](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3866b02dceb9bc7f937a599cabbc6e9b7452d39f3cc7f58a05a00571bfc60a0d2) | |  | | | • | [Microsoft Privacy](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3762a25e7447e5ca9ba29e553b9619135197f003b952f4818629dce77a6807a5a) | |  | | | • | [Microsoft Security Product Solution Centers](http://click.email.microsoftemail.com/?qs=9368efa76acefbc30f2e049c288f55a7d3e7dba71982512d9e20c76b123cc05767cac9e2f0c27b26) | | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Additional Resources   |  |  | | --- | --- | |  | | | • | [Trustworthy Computing Security and Privacy Blogs](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3ce89ee2f3832873683a73dab9210df29876c5b70efcd3119bbf5076fcbed6325) | |  | | | • | [Microsoft Security Intelligence Report](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3052c25f24fc1bc46fe0ee1f3970c6d2a7bd72cba2404d979c0d58c74df197c9f) | |  | | | • | [Microsoft Security Development Lifecycle](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3129eacf86f0a0a485a67df3d38a6bc5f50a797c7af28b63b41e0a7f427be6450) | |  | | | • | [Malware Response Guide](http://click.email.microsoftemail.com/?qs=9368efa76acefbc310c51d142e9c2700064ffd60f0a7d22d6f4a598c9061d18feeebc2404626ce18) | |  | | | • | [Security Troubleshooting and Support Resources](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3212f1c5750497156646cbe967c4452ae204065ed6caac5713a294ccc98766e06) | |  | | | • | [Trustworthy Computing Careers](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3abd98964a828594a0fc327a790b4001b43a336b9e82a39c092e1ec1f4b13c68d) | | | | |  | |  | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | |  | microsoft.com/about/twc | Trustworthy Computing |  | |  |  |  |  | | | |  | | --- | |  | |  | This is a monthly newsletter for IT professionals and developers–bringing security news, guidance, updates, and community resources directly to your inbox. If you would like to receive less technical security news, guidance, and updates, please subscribe to the Microsoft Security for Home Computer Users Newsletter.   © 2014 Microsoft Corporation [Terms of Use](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3bfbce8cd684f9fcba5873901f57d44c6a8d9873291a49a11ace63c6baf581371) | [Trademarks](http://click.email.microsoftemail.com/?qs=9368efa76acefbc368928dc16cb89efc4bada4306184ec72527bf3ca5b75c2b3ecff25eade574dfe)   Microsoft respects your privacy. To learn more please read our online [Privacy Statement](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3f0f8ad40c71c268326b0a230f12ba487dd8a72affe2c518408e717b5cf7d61b0).   If you would prefer to no longer receive this newsletter, please [click here](http://click.email.microsoftemail.com/?qs=9368efa76acefbc3a58cb8db0de8508f663d663453ac476645ae6f7f8ceec6a4e1a6b324719f99c3).   To set your contact preferences for other Microsoft communications [click here](http://click.email.microsoftemail.com/m_hcp.aspx?qs=0bb7f39debca1b0acb34d76711c30a6a96abb33fd8cde0008d7a64657972b3f57ed47edd117f26836cc535108b4fcce9bc5b1bb45d9f9373192536d2b1fa2efde7b55b7f038cad1957220a4cce906223abac9eaa936e16a3682aa21b953d235c12f93a35bf3caf3a).   Microsoft Corporation One Microsoft Way Redmond, WA 98052 USA | |  | |  |  |  |  | | |  | | |
|  |