February 2013

Microsoft Security Response Center

Key Points

- The Microsoft Security Response Center (MSRC) serves as Microsoft's single point of security coordination and communications and is led by some of the world's most experienced experts. The MSRC identifies, monitors, resolves, and responds to security incidents including vulnerabilities in Microsoft software. The MSRC also manages monthly security updates and publishes the Security Update Guide, Security Advisories, and a semi-annual Security Intelligence Report.

- Microsoft encourages reasonable, coordinated disclosure of vulnerabilities in its software and works to mitigate the exploitation of vulnerabilities through MSVR, MAPP, and the Microsoft Exploitability Index.

- Microsoft collaborates with the security community and other global partners to help create a more secure computing experience and a safer, more trusted Internet environment, including through BlueHat security briefings and ICASI.

BACKGROUND

Computer security is an ongoing, ever-changing challenge. Threats have become more complex and widespread as cyber criminals have developed sophisticated new ways to attack both large, interconnected systems and individual customers.

The Microsoft Security Response Center (MSRC), part of the Trustworthy Computing Group, was created to help keep pace with evolving threats and better protect customers against malicious attacks through timely security updates and authoritative guidance. The MSRC, led by some of the world's most experienced security experts, serves as Microsoft's single point of coordination and communication on security threats.

Each year, the MSRC manages over 100,000 reports of vulnerabilities in Microsoft software. It also draws on a worldwide network of security researchers and partners that closely monitors online security news lists and public forums. The MSRC identifies, monitors, responds to, and resolves security incidents following a four-step process when it receives information about a potential threat.

- **Evaluation**. The team evaluates the possible impact of the threat to customers.
- **Investigation**. MSRC experts gather enough information to reproduce the vulnerability and determine which products or services might be affected.
- **Severity rating**. The MSRC rates each vulnerability according to severity and the likelihood that it will be exploited.
- **Resolution**. The team decides whether to fix the problem with an immediate update to Microsoft software, or to resolve the issue in a future service pack or new product version.

The MSRC is committed to providing timely and prescriptive guidance and communicates with customers through a number of channels including blogs, bulletins, advisories, and webcasts.

- Since 2003, the MSRC has managed the release of software security updates company-wide to address vulnerabilities in Microsoft software. MSRC experts also write the Microsoft Security Bulletin, which is translated into multiple languages and published the second Tuesday of every month.

- In 2005, Microsoft introduced a supplement to these bulletins, Microsoft Security Advisories, which addresses security changes that may not require a bulletin but that may still affect customers' overall security.
- The MSRC developed the Microsoft Security Update Guide to help IT professionals better understand and maximize Microsoft security update release information, processes, and tools.
- The MSRC publishes the semi-annual Microsoft Security Intelligence Report, a comprehensive, up-to-date, and geographically relevant analysis of the cyber threat landscape of exploits, vulnerabilities, and malware. It draws on data from more than 600 million computers worldwide and some of the busiest online services on the Internet.

MICROSOFT APPROACH

Microsoft encourages reasonable, coordinated disclosure of vulnerabilities in its software and works to mitigate exploitation of them.

- **Microsoft Vulnerability Research (MSVR)** is a program through which Microsoft shares its collective experience and best practices in dealing with vulnerabilities within the security community. The goal is to foster positive change, which will ultimately improve the security ecosystem.
- **Microsoft Active Protections Program (MAPP)** offers security software providers information about vulnerabilities from the MSRC in advance of Microsoft's monthly security update. This advance warning gives these MAPP partners more time to build protections against the vulnerability so they can give their customers updated protections faster.
- **The Microsoft Exploitability Index**. In 2008, Microsoft launched the Index to help customers evaluate risk by providing information on the likelihood that a vulnerability addressed in a Microsoft security update will be exploited within the first 30 days of the update's release.

Microsoft collaborates with the security community and with partners to advance and improve security for customers and build a more trusted Internet.

- **BlueHat security briefings** are invitation-only conferences aimed at improving the security of Microsoft products. Microsoft security professionals and outside researchers come together to share ideas, and expertise about threats to global security.
- **Industry Consortium for Advancement of Security on the Internet (ICASI)**, co-founded by Microsoft, is a nonprofit corporation of leading IT companies that addresses international, multi-product security challenges to better protect the IT infrastructures that support the world's enterprises, governments, and citizens.

Helpful Resources

Microsoft Security Response Center
www.microsoft.com/msrc

MSRC blog
blogs.technet.com/msrc

Microsoft Security Intelligence Report
www.microsoft.com/sir

Microsoft Security Update Guide
aka.ms/msrc-guide

Microsoft Vulnerability Research (MSVR)
aka.ms/ms-msvr

Microsoft Active Protections Program (MAPP)
aka.ms/ms-mapp

Industry Consortium for Advancement of Security on the Internet (ICASI)
www.icasi.org

Microsoft Exploitability Index
aka.ms/Exploitability-Index

Microsoft Trustworthy Computing
www.microsoft.com/twc