Microsoft Security Response Center

Coordinated Vulnerability Disclosure: From Philosophy to Practice

MSRC / By msrc / April 19, 2011 / CVD

Last summer at the Black Hat security conference, we announced a philosophical shift in how we refer to vulnerability disclosure, called "Coordinated Vulnerability Disclosure" (CVD). Our intent was to focus on how coordination and collaboration are required to resolve security issues in a way that minimizes risk and disruption for customers. Since then, feedback from the broader security community has been generally supportive.

Today, we're providing more transparency and insight into our disclosure philosophy by announcing three updates to our disclosure practices – a CVD at Microsoft document, MSVR Advisories, and our internal corporate Disclosure of Vulnerabilities policy.

The **Coordinated Vulnerability Disclosure (CVD) at Microsoft** document clarifies how Microsoft responds not only as a vendor impacted by vulnerabilities in its products and services, but as a finder of vulnerabilities in third-party products and services, and as a coordinator of vulnerabilities that affect multiple vendors. Drawing upon our years of experience, we have seen that disclosing vulnerability details and/or exploits before a vendor has a chance to address the issue amplifies the risk of attacks.

As part of the Microsoft Vulnerability Research (MSVR) program, we are releasing the first **MSVR Advisories** for issues discovered by Microsoft in third party vendors' products. These issues were privately reported to the companies who have since provided remediation. Since it began operating in August 2008, MSVR has privately reported many vulnerabilities to other vendors to help improve the broader security ecosystem. MSVR Advisories further document our commitment to handling vulnerability disclosure in a coordinated way. Read more about our CVD philosophy and commitment to the security research community on Katie Moussouris' post on the **EcoStrat Blog.**

To help affirm Microsoft's commitment to the security of the computing ecosystem, Microsoft adopted an internal corporate **Disclosure of Vulnerabilities policy** that establishes protocols for employees to follow when a vulnerability is discovered in a third party product or service.

We believe the most effective approach to security is a comprehensive Security Development Lifecycle that reduces or mitigates vulnerabilities before a product is released. After a product or service is released, we feel security is a shared responsibility across the broad community. Collaboration between security researchers and vendors is ultimately about preventing attacks and protecting the computing ecosystem. By working together through coordinated efforts when vulnerabilities are identified, we can effectively minimize customer risk while a solution is developed. We encourage others to adopt this philosophy in the interest of creating a safer and more trusted internet for everyone.

Thank you,

Matt Thomlinson
General Manager, Trustworthy Computing Security

← Previous Post Next Post →

Search ...

Categories

BlueHat (182)

Japan Security Team (977)

MSRC (1,020)

Security Research & Defense (374)

Tags

advisory (60) ANS (47) Attack (45) Attack Vector (68) Black Hat (33) BlueHat Security Briefings (55) Community-based Defense (99) Defense-in-depth (39) EcoStrat (34) EMET (68) Exploitability (77) Internet Explorer (IE) (156) malware (59) Microsoft Office (81) Microsoft Windows (106) Mitigations (128) monthly bulletin release (48) rating (48) Risk Asessment (104) security (82) Security Advisory (134) Security Bulletin (133) security bulletin release (44) Security Bulletins (39) Security Conference Engagement (56) Security Ecosystem (52) Security Engineering (42) Security Research (82) Security Update (140) Security Update Webcast (46) Security Update Webcast Q & A (70) Update Tuesday (63) Webcast (37) Windows Update (68) Workarounds (74) Zero-Day Exploit (36) アドバイザリ (160) セキュリティ (54) セキュリティ情報 (463) セキュリティ更新 (90) ワンポイント (39) 啓発 (45) 展開 (45) 時事ネタ (42) 脆弱性 (248)

Recent Posts

Publishing CBL-Mariner CVEs on the Security Update Guide CVRF API

Security Update Guide Improvement – Representing Hotpatch Updates

BlueHat 2023: Applications to Attend NOW OPEN!

A Ride on the Wild Side with Hacking Heavyweight Sick Codes

Announcing the Microsoft Machine Learning Membership Inference Competition (MICO)

Archives

Select Month