Microsoft Security Response Center

Coordinated Vulnerability Disclosure Reloaded

BlueHat / By bluehat / April 19, 2011 / CVD, MSVR, Responsible Disclosure

Today on the MSRC Blog, Matt Thomlinson announced three new efforts to provide more transparency into Microsoft's vulnerability disclosure process. These included a Coordinated Vulnerability Disclosure (CVD) at Microsoft procedures document, the first release of MSVR Advisories on vulnerabilities that were discovered by Microsoft and fixed by affected vendors, and an internal employee disclosure policy.

The vulnerability disclosure debate has continued over the years with all sides seeking the best way to protect users. We believe the best way to improve software security is through comprehensive Security Development Lifecycle (SDL) programs that build security into software from the very beginning. For vulnerabilities that remain after software is released, we feel that disclosure of vulnerability details should be done in a way that allows vendors an opportunity to address the issues without amplifying risk.

In our experience as finders and coordinators, we know that disclosing vulnerabilities to a vendor can be a complex process. This is why we developed the Microsoft Vulnerability Research (MSVR) program as a way for our employees to report vulnerabilities they find to affected vendors.

We understand that there are differing approaches to vulnerability disclosure. Even if finders do not share our disclosure philosophy, we appreciate any information finders are willing to share with us. Our hope is that finders will give us the opportunity to address the issue comprehensively with a fully tested update before releasing technical details publicly. We hope our transparency with our disclosure process encourages more finders to work with us who may not have otherwise.

We've listened to the security community, including security researchers, vendors and CERTs, in documenting our approach to disclosure. We'd like to thank the following people for reviewing our Coordinated Vulnerability Disclosure at Microsoft document. If you have comments or opinions, we'd like to hear from you. Please follow us on Twitter at @msftsecresponse or me at @k8em0.

– Katie Moussouris, Senior Security Strategist, MSRC

Microsoft thanks the following people for reviewing our Coordinated Vulnerability Disclosure procedures document:

Bryan Burns, Distinguished Engineer, Juniper Networks

Arturo 'Buanzo' Busleiman, Independent Security Consultant

Steve Christey, CVE Editor, MITRE

Dave Dittrich, Security Engineer/Researcher, Applied Physics Laboratory, University of Washington

Jussi Eronen, Infosec adviser, CERT-FI

Ian Glover, President, Council of Registered Ethical Security Testers (CREST)

Jake Kouns, CEO, Open Security Foundation

Zach Lanier, Intrepidus Group

Marc Maiffret, Chief Technology Officer, eEye Digital Security

Art Manion, CERT Vulnerability Analysis Team

Steve Manzuik, Director of Security Research, Leviathan Security Group

Charlie Miller, Independent Security Evaluators

Toshio Miyachi, Board Member, JPCERT Coordination Center

Bruce Monroe, Senior Information Security Specialist, Intel

Mike Prosser, Symantec Product Security Team

Ryan Permeh, Manager of Product Security, McAfee

Marsh Ray, Senior Software Development Engineer, Phonefactor

Russell Smoak, Sr Director / GM Security Research and Operations, CISCO Services

Chris Wysopal, Chief Technology Officer, Veracode

← Previous Post Next Post →

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