Sicherheitsanfälligkeit in Windows Shell kann Remotecodeausführung ermöglichen

From:	Sehenswürdigkeiten Außerdem
To:	altă surpriză, Sehenswürdigkeiten Außerdem, EDGE01 RTF01, EDGE02 RTF02, EDGE03 RTF03, EDGE04 RTF04, EDGE05 RTF05, Merkés François, QA_ATI, Shane O'Malley, Ανάπτυξης Ευρωπλάνο, Проверка драйверы
Date:	2010/08/02 16:12
Subject:	Sicherheitsanfälligkeit in Windows Shell kann Remotecodeausführung ermöglichen
Attachments:	TEXT.htm, Verknüpfungen.rtf

Allgemeine Informationen

sID='2l1-ERB'Kurzzusammenfassung

Microsoft untersucht derzeit Meldungen über begrenzte, gezielte Angriffe, bei denen eine Sicherheitsanfälligkeit in Windows Shell ausgenutzt wird, eine Komponente von Microsoft Windows. Diese Empfehlung enthält Informationen zu den anfälligen Versionen von Windows sowie zu Problemumgehungen und schadensbegrenzenden Maßnahmen für dieses Problem.

Die Sicherheitsanfälligkeit liegt vor, weil Windows Verknüpfungen falsch analysiert, sodass schädlicher Code ausgeführt werden kann, wenn das Symbol einer speziell gestalteten Verknüpfung angezeigt wird. Diese Sicherheitsanfälligkeit kann lokal durch ein schädliches USB-Laufwerk oder von einem Remotestandort aus über Netzwerkfreigaben und WebDAV ausgenutzt werden. Eine Ausnutzung kann auch in bestimmten Dokumententypen enthalten sein, die eingebettete Verknüpfungen unterstützen.

Microsoft arbeitet derzeit an der Entwicklung eines Sicherheitsupdates für Windows, um diese Sicherheitsanfälligkeit zu beheben.

Wir arbeiten aktiv mit Partnern in unserem Microsoft Active Protections Program (MAPP) zusammen, um Informationen bereitzustellen, mit denen sie einen umfassenderen Schutz für ihre Kunden

Property	Value
Message id	4C56EE5D.dom1.po1.100.1346769.1.7F.1
Message Path	xml/Mailbox/4C56EE5D.dom1.po1.100.1346769.1.7F.1.xml
From	Sehenswürdigkeiten Außerdem
Display Name	Sehenswürdigkeiten Außerdem
Email	Außerdem@smt.qa.com
UUID	526E4940-0A79-0000-961A-B6E75AD0D8A9
Reply To	Außerdem@smt.qa.com
Text	Sehenswürdigkeiten Außerdem

Property	Value
Message id	4C56EE5D.dom1.po1.100.1346769.1.7F.1
To	altă surpriză; Sehenswürdigkeiten Außerdem; EDGE01 RTF01; EDGE02 RTF02; EDGE03 RTF03; EDGE04 RTF04; EDGE05 RTF05; Merkés François; QA_ATI; Shane O'Malley; Ανάπτυξης Ευρωπλάνο; Проверка драйверы
CC	
Subject	Sicherheitsanfälligkeit in Windows Shell kann Remotecodeausführung ermöglichen
Scheduled date	2010-08-02 16:12:13
Creation date	2010-08-02 16:12:13
Modified date	2010-08-19 13:19:29
Delivered date	2010-08-02 16:12:13
Message size	1256
Attachments	2
Attachment	TEXT.htm
Name	TEXT.htm
Content ID	4C56EE5D.dom1.po1.200.20000C1.1.62.1@45:4C56EE5D.dom1.po1.100.1346769.1.7F.1@1:7.dom1.po1.100.0.1.0.1@16
Is Inline	false
Type	file
Size	1716
Date	2010-08-02 12:12:12
CA	accounts\test German@ßÜüÖöéÄä.po1.dom1\content\9E\9E9D84B6C84311E293B4309870EFE0AD5AF919F51377A47519C0E7630DD4F2E0AAFFA96F
Hash	9E9D84B6C84311E293B4309870EFE0AD5AF919F51377A47519C0E7630DD4F2E0AAFFA96F
Attachment	Verknüpfungen.rtf
Name	Verknüpfungen.rtf
Content ID	4C56EE5D.dom1.po1.200.20000C1.1.63.1@45:4C56EE5D.dom1.po1.100.1346769.1.7F.1@1:7.dom1.po1.100.0.1.0.1@16
Is Inline	false
Type	file
Size	2477
Date	2010-08-02 12:12:12
CA	accounts\test German@ßÜüÖöéÄä.po1.dom1\content\A5\A5FBD35AED3EC7A2664A416123E390BC16D2257544B3974A9C898C1D1BD43E1688055C84

Property	Value
Message id	4C56EE5D.dom1.po1.100.1346769.1.7F.1
Hash	A5FBD35AED3EC7A2664A416123E390BC16D2257544B3974A9C898C1D1BD43E1688055C84
Recipients	12
Recipient	altă surpriză
Display Name	altă surpriză
Email	altă@smt.qa.com
UUID	B796BBF0-01FE-0000-BC4B-AAA2BC7891B1
Distribution Type	TO
Recipient Type	User
Recipient	Sehenswürdigkeiten Außerdem
Display Name	Sehenswürdigkeiten Außerdem
Email	Außerdem@smt.qa.com
UUID	526E4940-0A79-0000-961A-B6E75AD0D8A9
Distribution Type	TO
Recipient Type	User
Recipient	EDGE01 RTF01
Display Name	EDGE01 RTF01
Email	EDGE01@smt.qa.com
UUID	3FAA9740-0200-0000-BC4B-AAA2BC7891B1
Distribution Type	TO
Recipient Type	User
Recipient	EDGE02 RTF02
Display Name	EDGE02 RTF02
Email	EDGE02@smt.qa.com
UUID	4FCE5DA0-0200-0000-BC4B-AAA2BC7891B1
Distribution Type	TO
Recipient Type	User
Recipient	EDGE03 RTF03
Display Name	EDGE03 RTF03
Email	EDGE03@smt.qa.com
UUID	61B271A0-0200-0000-BC4B-AAA2BC7891B1
Distribution Type	TO
Recipient Type	User
Recipient	EDGE04 RTF04
Display Name	EDGE04 RTF04
Email	EDGE04@smt.qa.com
UUID	7484DD40-0200-0000-BC4B-AAA2BC7891B1
Distribution Type	TO
Recipient Type	User
Recipient	EDGE05 RTF05

Property	Value
Message id	4C56EE5D.dom1.po1.100.1346769.1.7F.1
Display Name	EDGE05 RTF05
Email	EDGE05@smt.qa.com
UUID	871E1070-0200-0000-BC4B-AAA2BC7891B1
Distribution Type	TO
Recipient Type	User
Recipient	Merkés François
Display Name	Merkés François
Email	François@smt.qa.com
UUID	BB6C1BF0-02C4-0000-9410-6A16583C76B2
Distribution Type	TO
Recipient Type	User
Recipient	QA_ATI
Display Name	QA_ATI
Email	QA_ATI@smt.qa.com
UUID	079EA710-0205-0000-BC4B-AAA2BC7891B1
Distribution Type	TO
Recipient Type	SystemGroup
Recipient	Shane O'Malley
Display Name	Shane O'Malley
Email	Shane@smt.qa.com
UUID	01B93ED0-15A3-0000-9BFE-8367BDA0E416
Distribution Type	TO
Recipient Type	User
Recipient	Ανάπτυξης Ευρωπλάνο
Display Name	Ανάπτυξης Ευρωπλάνο
Email	Ευρωπλάνο@smt.qa.com
UUID	413567E0-01FE-0000-BC4B-AAA2BC7891B1
Distribution Type	TO
Recipient Type	User
Recipient	Проверка драйверы
Display Name	Проверка драйверы
Email	Проверка@smt.qa.com
UUID	16171620-01FF-0000-BC4B-AAA2BC7891B1
Distribution Type	TO
Recipient Type	User
Expire	0
Delay delivery until	0
Delegated	false
Archived	false
Read	true

Property	Value
Message id	4C56EE5D.dom1.po1.100.1346769.1.7F.1
Deleted	false
Opened	true
Completed	false
Security	Normal
Box type	Inbox
Return notification when opened	false
Return notification when deleted	false
Return notification when completed	false
Return notification when declined	false
Return notification when accepted	false
Archive Version	2008.1
Internal ID	4C56EE5D.dom1.po1.100.1346769.1.7F.1@1:7.dom1.po1.100.0.1.0.1@16
Name	
Source	received
Class	Public
Account	test German@ßÜüÖöéÄä.po1.dom1
Location ID	1295973731638
Class Name	GW.MESSAGE.MAIL
Original Subject	
Personal Subject	
Enclosing Folders	1
Folder	Mailbox
ID	7.dom1.po1.100.0.1.0.1@16
Name	Mailbox
Type	Mailbox
System	true
Share Type	NotShared