

Visa Data Security Alert

Targeted Hospitality Sector Vulnerabilities

November 06, 2009

To promote the security and integrity of the payment system, Visa is committed to helping clients and payment system participants better understand their responsibilities related to securing cardholder data. As part of this commitment, Visa issues Data Security Alerts when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Memory Parsing Vulnerability

A vulnerability that was identified previously by a Visa approved forensic company, in a Data Security Alert on memory parsing (October 2, 2008) is actively targeting and being exploited within the hospitality industry. This vulnerability is carried out by hackers in which they install debugging software on point-of-sale (POS) systems in order to extract full magnetic stripe data from volatile memory, otherwise known as "RAM."

To ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS), all systems including POS systems must not store sensitive authentication data (i.e., full magnetic stripe data, CVV2, PIN data). However, the increasing use of debugging tools that parse data from volatile memory suggests attackers may have successfully adapted their techniques to obtain payment card data that is not written to POS system disks. This method of data extraction from memory is of particular concern since unencrypted data is commonly written to volatile memory during the transaction process. Hackers may utilize tools (e.g., PsExec) to execute the program remotely.

Other Vulnerabilities Identified

Visa has also seen cases in which hackers with full access to the system enable debug mode on payment applications to obtain full magnetic stripe data from the system. For this type of attack, debugging software is not necessary since the payment application has the option to enable debug mode for troubleshooting purposes. Contact your application vendor to ensure security controls are properly configured to prohibit unauthorized modification to such administrative level settings.

Based on Visa's computer forensic investigations, hackers are gaining unauthorized access to POS environments as a result of an entity's insecure remote management solutions or poor network configuration.

Visa strongly urges stakeholders share this alert with their information security teams and review their systems including POS and remote management applications for weak passwords, unknown debugging software programs and ensure networks and the overall payment environment are securely configured and maintained in accordance with the PCI DSS.

Recommended Mitigation Strategy

The following security practices should be implemented to help mitigate these security risks:

- Secure remote access connectivity. See Visa Data Security Bulletin "Top Three POS System Vulnerabilities," dated November 21, 2006, available at www.visa.com/cisp.
- Implement a secure network configuration, including egress and ingress filtering to **only** allow the ports/services necessary to conduct business. See Visa Data Security Alert "Improperly Segmented Network Environment," dated October 31, 2006, available at www.visa.com/cisp.
- Utilize host-based Intrusion Detection Systems (IDS) and actively monitor logs of network components, including IDS and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses.
- Use packet sniffers legitimately to detect network intrusion attempts or suspicious activity on a network.
- Organizations which use MPLS topology for shared network and protocol switching should take steps to secure their MPLS environments. See *Complete Guide for Securing MPLS Networks* available at <http://whitepapers.zdnet.com/abstract.aspx?docid=383671>.
- Ensure all anti-virus, anti-malware and anti-spyware software programs are up-to-date.
- Encrypt cardholder data anywhere it is being stored, and consider implementing a data field encryption solution to directly address cardholder data in transit. See Visa Data Security Bulletin "Visa Best Practices for Data Field Encryption, Version 1.0," dated October 6, 2009, available at www.visa.com/cisp.
- Review systems to ensure removal of unnecessary software, services and tools (e.g., PsExec).
- Implement file integrity monitoring and secure all systems so unauthorized software cannot be installed.
- Work with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration.
- Implement least privileges necessary on user and application accounts to prevent execution of malware and modification to payment application settings.
- If you detect a suspected or confirmed security breach, notify your acquiring bank immediately. For more information, please refer to Visa's *What To Do If Compromised*, available at www.visa.com/cisp under the "If Compromised" section. You can also contact Visa Fraud Control and Investigations at usfraudcontrol@visa.com or (650) 432-2978.

See Appendix A for a list of debugging software and other executables related to this vulnerability.

Visa Data Security Alert

Appendix A: Memory Parsing Vulnerability – Searchable Files



Filename/Variant	Function	File size (bytes)	MD5/SHA-1 hash
ANSI.dll	Perl2Exe-related DLL	-	-
API.dll	Perl2Exe-related DLL	32,883	224D11EC6F4F6475096A50D51E187AD5
BAND F.exe	Sniffer	94,208	a6f3372ab4b706d703627becaa6d2aeb
band fud.exe	Sniffer	114,688	274ab0264d62d680576d16e13f9f8276
bifro f.exe	Sniffer	143,360	45d721df8d8bbeb2364022f272accce5
Bios12.rom	Log file with cardholder data	-	-
BugSlayerUtil.dll	Backdoor and ServU components	36,864	7fa6a4eb44c09ccd324ce804d3323010
compenum.exe	Network scanner that outputs a list of accessible systems	54,272	bcc61bdf1a2f4ce0f17407a72ba65413
Config.dll	Backdoor and ServU components	65,536	812cb13e98ada09a0d517f38475e11c5
console.exe	Rar installer	1,068,076	DAB75CB15DDD2C6C68154007F6A90F81
	-	96,256	8987642802D03FA63707524B924B0AD1
convertxdccfile.exe	Backdoor and ServU components	131,072	2d58e0a7f01a08b41c74838089653556
csrss.exe	Backdoor and ServU components	434,176	2f384e163c46bd7617d7e9ef603cbee6
csrsvc.exe	Memory dumper	75,264	1f9d0d200321ad6577554cc1d0bb6b69
			ec137291dd52a3a2de246f22d3cbc7f0
			8bfa2c3e089c10bc39ae6d0d41e4acf211318db4
		74,752	504EE1C0BDEA9C80307860BE9A8356DE
			03839FFF84950BBD2E33591C7B75398F
			b4f28e51ec62712951ee6292936768c8
		76,288	79E417BCE7176C597CEF4CF6C3C5087D
			4B254B90F61D82194672B0CE55B020DA
		-	1F9D0D200321AD6577554CC1D0BB6B69
		-	76B0C7AE7D652DF025BD6E001226F76C

Filename/Variant	Function	File size (bytes)	MD5/SHA-1 hash
	Dump virtual memory from specifically identified processes, including CCS.exe	74,752	b4f28e51ec62712951ee6292936768c8
		-	f3f932ba44007e130c61da789f72163b
Cwd.dll	Perl2Exe-related DLL	20,573	07944E74E8BCC07DFA7CC7E4946BB865
cygcrypt-0.dll	Backdoor and ServU components	8,192	fcaaad96b6b4e41dbaf9076109dcb964
cygwin1.dll	Backdoor and ServU components	1,875,968	e8cd5a2ba5d93acce6c28c26bf5717fb
		1,142,784	2852ff9d8f43590d3963b298f9a6492e
dirmon.chm	Output file from track data parser programs	39,560	ac15d275d4d01c453aab907da7051f81
	Log file with cardholder data	-	-
dnsmgr.exe	Track data memory parser	1,162,117	bf27e87187c045e402731cdaa8a62861
	Perl script 'compiled' via Perl2Exe to parse memory dump from csrsvc.exe for track data (writes to dirmon.chm)	1,162,121	04da2210591489494b498944084d47e6
		-	74EB29A6B9DCFCED478EE2BB867B7B23
		-	55b9ba26bf854e9f2893841129afc457
		1,162,103	FC28642F5EF83F787C5B8B251597FBC2
1,162,136	DBE4D7E8EC8851091A59724154C4102		
Dr.MOT test.exe	Sniffer	131,072	0f4a32737cb7a749fbfe3c3677d46075
dump.bat	Batch file installs memory dumper program on a single computer	273,408	9393aaf96f3fc25bfcc6649e33edc560
ent.exe	Essential NetTools network scanner	358,400	defd991b647811e8e8e5591365e3be41
EXEC.exe	Backdoor and ServU components	61,440	a59eb13591325bb6c260ac8348bd63e9
far.exe Far.exe	DOS based file manager used by attacker	620,032	d1d9c26a77beb82b13c82e854042dc92
	Archive program	586,752	ee7d411f47b13fb204a188fc37e7fc61
Fcntl.dll	Perl2Exe-related DLL	24,673	7F26A42C1D0FC8733755F76B47DF8EFC
File.dll	Perl2Exe-related DLL	82,024	240CF55A6B41469BC9EDA49E45DE7C79
get2.exe	GET2 Penetrator	49,152	73ba6f159e752705ed2cde6953769a9b
giohack.bat	Backdoor and ServU components	65,536	9f815b15264ed9ee191d9260ee66bb7a
host32edu.exe	Backdoor trojan	66,303	6c9e01933aa88894f476d690666dc403
inetinfo.chm	Encrypted log file	-	-

Filename/Variant	Function	File size (bytes)	MD5/SHA-1 hash
	with cardholder data		
install.bat	Batch file that installs WinMgmt as a Windows service	44,032	a7c24031cae3f29ec0c30d220c52a087
	Backdoor and ServU components	342,016	b53fece9590f1d594a5837d8411bff4c
IO.dll	Perl2Exe-related DLL	24,667	4A4D77ECC2E7E0938FEBF344A5F6DA8A
ioTar.bat	Backdoor and ServU components	684,032	7401d1471dc0fb50570ccf534dc9651a
ioTar.exe	Backdoor and ServU components	262,144	ea9149dff18b06de8ba36a5d8e8f322
k.exe	Backdoor and ServU components	131,072	d17da0ce1754e2f0548f0b258f6441d2
kill.exe	Used for killing processes	9,488	DE2AA4542B66DAD92FA37D9E9CB8A5AC
lan1.exe	Rar installer	2,930,988	6B0FAD39235BD1D5B3A8A8376FA3E099
lanst.exe	-	1,528,675	A63D6203D1D7568868EBE7521406B057
libeay32.dll	Backdoor and ServU components	675,840	7d7a08727bdfac87b7f8c8ae7a08c279
locked.exe	Backdoor and ServU components	372,736	9977cb9c7ded7fa4f0fb01a689c777b9
mdirmon.exe	Memory dumper	1,162,251	70CB68C3CD4A1744157137276C80B884
MemPDumper.exe	Memory dumper	75,776	dbaab511f2210228e41c3ffdbe5d3fce
msdgr.exe	Sniffer	114,688	274ab0264d62d680576d16e13f9f8276
ms-java.exe	Backdoor and ServU components	57,344	ea2e9e72f5bc8ac2549b325a757d321d
Mssvc.exe	Backdoor and ServU components	2,146,304	349994e52cb43df1528c6f79a4e0db6f
new pi fpack.exe	Sniffer	49,152	8c93c7a13fd0c0d4dd78bda9a6422025
p2x588.dll	Perl2Exe-related DLL		5BBF8F03CD47A4AE4D5B9A7F56A080AB
Packetsniffer.exe	Packet Sniffer	58,131	f44527cdeb1c7c1b8348f39180a18a98 3dce8b0402d9404f6c2b3a3f2eee6f0a
parser.exe	-	1,496,848	739DEE364F220BFA7E600A81F5F9C916
ph.exe	Keylogger components	25,088	01bbe511da55597af1184489ab4912a6
php4ts.dll	Backdoor and ServU components	1,396,736	d31b6d08abc55f5ebcfcdca86d5090f47
play.bat	File calls install.bat file to install memory dumper on multiple systems	80,896	fc37de3b9b1c831a52a836b7a2f2695
POSIX.dll	Perl2Exe-related DLL	-	-
psexec.exe	Sysinternal tool	135,168	579b43e13294eb85faa7c28b470b19c1

Filename/Variant	Function	File size (bytes)	MD5/SHA-1 hash
	used to run process on remote machines		
psk.exe	PC spy keylogger	1,518,740	f872e93114f2d258ca6b4175281dca57
radminshare.exe	-	53,248	E371DA3542E12045AE2BEBA2F088E7AC
Ramddumper.exe	Memory dumper	197,120	561D8CBD96C903F82B03D7936031BFC5
rar.exe	Archive program	302,080	8061445DAC265AC6F9F7151B06519126
rdasrv.exe	Memory parsing malware. Track 1 and 2 regular expression embedded on malware. Output file with credit card data labeled data.txt. Malware uses SCM	117,760	d9a3fb2bfac89fea2772c7a73a8422f2
rdelservice.exe	Used for removing services	53,760	41C8331A04E912C9D2CD9FCC87837F7C
re.dll	Perl2Exe-related DLL	106,587	495887BD80A0F04FF5AFAAD4035B9423
REC.bat	Backdoor and ServU components	65,536	0c7884745ee230b320ca00a24cbde5b5
rpcsrv.exe	Memory dumper	151,552	51d08d0d822f29ca2d426cf6acfc349c
		-	8265C4D2FAE4C0614092EC47BB9098DC
run.bat	Backdoor and ServU components	123,904	23459d9b1ddf833f7f9d3a28174223ba
server.exe	Proxy	888,832	e02d4cc6ec3b7907b35d9456ab092da3
service.dll	Backdoor and ServU components	377,856	f4beedf02d88585424fd8ff751252732
service.exe	Backdoor and ServU components	143,360	91009b6d27c4692ff57f2bc574f9f3fd
shareenum.exe	Network scanner that outputs a list of accessible shares	53,248	3ca6ec07c6b840e7a256d09839ba0c4f
spy.log	Keylogger components	451,584	-
spydll.dll	Keylogger components	49,152	63c84d547940efa3a60e24aff89f04e9
ssleay32.dll	Backdoor and ServU components	151,552	35e95d8777732a6cbd82b01b90e06df9
svchost.exe SVCHOST.EXE	Sniffer	360,448	56ede51c4af1840cb62eaff237f026e6
	Backdoor	610,304	ee23d3c0de12c1644f0ed8abc818aca1
sys32.exe	IRC client	9,216	cddb6f0a7add0a8c36c4d3ec7b637e9f
tasken.exe	Sniffer	94,208	a6f3372ab4b706d703627becaa6d2aeb
taskmgr.exe	Backdoor and ServU components	266,240	ef053224ae63d19c2928be406ce24b1f

Filename/Variant	Function	File size (bytes)	MD5/SHA-1 hash
tcl84t.dll	Backdoor and ServU components	831,488	3bb3ccba6d97c23dd79d15f738b41907
tzoLibr.dll	Backdoor and ServU components	36,864	c39396c57353dd2a379d2f5a2cb1435f
Util.dll	Perl2Exe-related DLL	28,772	E56800466B7DD6283A4F2AE7178A7B70
Win32.dll	Perl2Exe-related DLL	41,057	78C16D8A7D6E0DB9DBE580C9F125EEAC
windowsupdate.exe	Keylogger components	20,992	770cf74f9ec0ca12d501a43891ca56bb
wings.exe	Sniffer	49,152	8c93c7a13fd0c0d4dd78bda9a6422025
winmgmt.exe WinMgmt.exe	Calls csrssvc.exe and dnsmgr.exe and runs an interactive command shell on tcp port 3373	66,048	3e19ef9c9a217d242787a896cc4a5b03
	Install the Windows Management Help Service service, launch "start /min csrssvc.exe" and "start /min dnsmgr.exe"	-	6ad25d1cb1bb86186d2a516dd0af6da9
	Install the Windows Management Help Service service, launch "start /min csrssvc.exe" and "start /min dnsmgr.exe"	66,048	c95a12932b1bfc85270f3fedc9d7b146
winslogon.exe	Sniffer	49,152	8c93c7a13fd0c0d4dd78bda9a6422025