



## PCI DSS – Quarterly ASV Scan – Detailed Report

**Post Office Limited**

**Fujitsu**

**October 2015 - Version 1.0**



NCC Group  
Managed Security Monitoring Services  
NCC Group plc  
Manchester Technology Centre  
Oxford Road,  
Manchester  
M1 7EF

[www.nccgroup.com](http://www.nccgroup.com)

Prepared by:  
Alex Blood  
Lead Technical Account Manager

Tel:   
Email:





# Table of Contents

<i>Area</i>	<i>Page Number</i>
<i>Table of Contents</i>	<i>2</i>
<i>Report Introduction</i>	<i>3</i>
<i>Report Details and Quality Assurance</i>	<i>4</i>
<i>ASV Scan Report Attestation of Scan Compliance</i>	<i>5</i>
<i>PCI ASV Scanning Methodology</i>	<i>7</i>
<i>Executive Summary</i>	<i>8</i>
<i>Vulnerabilities Noted for Each IP</i>	<i>10</i>
<i>- Special Notes</i>	<i>12</i>
<i>Vulnerabilities - Detailed</i>	<i>16</i>
<i>Vulnerabilities - Solutions</i>	<i>22</i>
<i>Open Ports List</i>	<i>26</i>



# Report Introduction




On completion of the PCI DSS ASV Scans conducted for Post Office Limited, NCC Group is pleased to present the findings in this report. This report aims to concisely outline the results collected during testing and to define specific actions Post Office Limited may take in order to mitigate issues identified and bring the systems in line with the PCI DSS requirements.

## Definitions of Risk Ratings

NCC Group have adopted the Common Vulnerability Scoring System. CVSS is a vendor independent, industry open standard. It is designed to convey vulnerability severity, help determine urgency and priority of response. The table below gives a key to the icons and symbols used through this report to provide a clear and concise risk scoring system.

It is designed to convey vulnerability severity, help determine urgency and priority of response. The table below gives a key to the icons and symbols used through this report to provide a clear and concise risk scoring system.

It should be stressed that the overall business risk posed by any of the issues found in any test is outside our remit. This means that some risk may be reported as high from a technical perspective but may, as a result of other controls unknown to us, be considered acceptable.

CVSS Score	Severity	Description	Symbol	Implication
7.0 Through 10.0	High	Trojan horses, Remote command execution, File read exploit, directory browsing and Denial of Service (DoS) where command execution is possible		An area or finding where HIGH/MEDIUM attention is required, and there may be significant risk <b>These are not compliant with the PCI DSS</b>
4.0 Through 6.9	Medium	Sensitive information can be obtained by hackers on configuration.		
0.0 Through 3.9	Low	Information can be obtained by hackers on configuration		An area or finding that should be noted by IT Security management and appropriate action taken.

Certainty Definition	Description
Proven Vulnerable	There is evidence that this is 100% genuine issue. This evidence is provided in the probe output section.
Version Vulnerable	From the information gathered during the scan, this vulnerability cannot be verified without exploitation or without evidence that the system is patched or configured securely.
Potentially Vulnerable	This is where evidence of the vulnerability is found but cannot be confirmed as accurate.



# Report Details and Quality Assurance

## Quality Assurance

### Document Details

Document Name	Post Office Limited_PCI Report_Oct_FJ_2015.docx
Date	02 October 2015
NCC Group Document Reference	POFF-049

Version	Date	Author	QSA Review
0.1	02 October 2015	Alex Blood	
1.0	02 October 2015		Thomas McDonald

## Document Usage

This report is intended for use only by the parties to the agreement noted above. If you have received this report in error, please call the Penetration and Security Testing department on: **GRO**

This report may not be reproduced by any means in whole or in part without the approval of NCC Group.

This document contains detailed commercial, financial and legal information, which is confidential and commercially sensitive. The release of such information will be prejudicial to the commercial interests of NCC Group and therefore should not be disclosed as a response to a Request for Information under the Freedom of Information Act 2000.

The document may also not be reproduced or the contents transmitted to any third party without the express consent of NCC Group. NCC Group gives no warranty and makes no representation in respect of the contents of this report.



# ASV Scan Report Attestation of Scan Compliance



Scan Customer Information		Approved Scanning Vendor Information	
Company: Post Office Limited		Company: NCC Group – Managed Security Services – PCI ASV	
Contact: Richard Miller	Title: Technical Security Assurance Manager	Contact: Alex Blood	Title: Qualified ASV Employee (QAE 900-518)
Telephone: <span style="border: 1px dashed black; padding: 0 5px;">GRO</span>	E-Mail: <span style="border: 1px dashed black; padding: 0 5px;">GRO</span>	Telephone: <span style="border: 1px dashed black; padding: 0 5px;">GRO</span>	E-Mail: <span style="border: 1px dashed black; padding: 0 5px;">GRO</span>
Business Address:	Finsbury Dials 20 Finsbury Street London EC2Y 9AQ	Business Address:	NCC Group Manchester Technology Centre Oxford Road Manchester M1 7EF
URL:	www.postoffice.co.uk	URL:	www.nccgroup.com

## Attestations

### Scan Customer Attestation

**Post Office Limited** attests on **01 October 2015** that this scan includes all components which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. **Post Office Limited** also acknowledges the following:

1. Proper scoping of this external scan is my responsibility, and
2. This scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

### ASV Attestation

This scan and report was prepared and conducted by **NCC Group – Managed Security Services – PCI ASV** under certificate number **3928-01-09**, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide.

**NCC Group – Managed Security Services – PCI ASV** attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of

1. Disputed or incomplete results,
2. False positives and
3. Active scan interference.

This report and any exceptions were reviewed by Alex Blood. QAE 900-518, Signed:

**GRO**

# ASV Scan Report Attestation of Scan Compliance



## Status and Scope of Testing

Post Office Limited requested that NCC Group perform a PCI DSS ASV scan on the following infrastructure and applications which have been identified as being in scope of PCI DSS. This assessment involved the following IP addresses and applications:

- Number of unique components scanned: **14**
- Number of identified failing vulnerabilities: **0**
- Number of components found by ASV but not scanned because scan customer confirmed components were out of scope: **0**
- This assessment commenced on the 01 October 2015. This Certificate expires 90 days from reportdate (30 December 2015).
- NCC Group has determined that Post Office Limited is **COMPLIANT** with the PCI scan validation requirement.

This assessment involved the following IP addresses and applications:

IP Address	Hostname
194.176.201.49-49 194.176.201.53-53 194.176.219.225-227 194.176.219.241-245 62.60.125.113-113 62.60.125.97-99	None

NCC Group performed an ASV scan of the scoped network infrastructure and applications. Specifically the work included:

-



# Executive Summary

## PCI DSS ASV Compliance Test results

Scan Information			
Scan Customer Company:	Post Office Limited	ASV Company:	NCC Group - Managed Security Services - PCI ASV
Date Scan Was Completed:	01 October 2015	Scan Expiration Date:	30 December 2015

The severity levels of the vulnerabilities found within live hosts are detailed below:

URL/IP Address	Highest CVSS Base Score	Severity Rating	Compliance Status	Page
62.60.125.97	0.0	✓ LOW	✓ PASS	10
62.60.125.98	0.0	✓ LOW	✓ PASS	10
62.60.125.99	0.0	✓ LOW	✓ PASS	10
62.60.125.113	0.0	✓ LOW	✓ PASS	11
194.176.201.49	0.0	✓ LOW	✓ PASS	11
194.176.201.53	0.0	✓ LOW	✓ PASS	11
194.176.219.225	0.0	✓ LOW	✓ PASS	11
194.176.219.226	0.0	✓ LOW	✓ PASS	11
194.176.219.227	0.0	✓ LOW	✓ PASS	11
194.176.219.241	0.0	✓ LOW	✓ PASS	11
194.176.219.242	0.0	✓ LOW	✓ PASS	11
194.176.219.243	0.0	✓ LOW	✓ PASS	11
194.176.219.244	0.0	✓ LOW	✓ PASS	11
194.176.219.245	0.0	✓ LOW	✓ PASS	11

Hosts where the operating system has been identified are:

IP Address	Operating System	Architecture	Vendor	Certainty
------------	------------------	--------------	--------	-----------





# Executive Summary

**No Hosts Could be Fingerprinted**

Note: Hosts not listed above were not able to be fingerprinted.





# Vulnerabilities Noted for Each IP

The table below outlines all identified vulnerabilities for each scanned host along with the risk of said vulnerability. Please see the vulnerability details section regarding CVSS Score amendment notes when Exceptions, False Positives, or Compensating Controls have been provided to the ASV.

Please note that Denial of Service (DoS) issue are reported below as required however these are not marked as a Fail as per the PCI ASV programme guidelines. However it is strongly recommended that all DoS issues be addressed to further enhance the security of your network perimeter. One exception to not recording DoS issues as a PCI ASV FAIL is where a DoS issue is co-present with another separate significant issue for a given vulnerability single vulnerability. By way of an example in several vulnerabilities a DoS issue or a Remote Code Execution issue may be possible a outcome for the identified single vulnerability. In this example case as remote code execution is also possible as an alternative to the DoS outcome the issue remains in force, there are many other examples where DoS issues co-exist as outcomes with other significant weaknesses as described above and in these cases they will be recorded as a PCI ASV FAIL.

62.60.125.97							✓
Severity Level	CVSS Base Score	Compliance Status	Port	Service	Vulnerability Name	Exceptions, False Positives, or Compensating Controls, Noted by ASV for Vulnerability	Page
✓ LOW	0.0	✓ PASS	N/A	N/A	ICMP timestamp response (CVE-1999-0524)	None Noted.	16
✓ LOW	0.0	✓ PASS	161/udp	SNMP	SNMP v2 GetBulk Traffic Amplification	None Noted.	16

62.60.125.98							✓
Severity Level	CVSS Base Score	Compliance Status	Port	Service	Vulnerability Name	Exceptions, False Positives, or Compensating Controls, Noted by ASV for Vulnerability	Page
✓ LOW	0.0	✓ PASS	N/A	N/A	ICMP timestamp response (CVE-1999-0524)	None Noted.	17
✓ LOW	0.0	✓ PASS	161/udp	SNMP	SNMP v2 GetBulk Traffic Amplification	None Noted.	17

62.60.125.99							✓
Severity Level	CVSS Base Score	Compliance Status	Port	Service	Vulnerability Name	Exceptions, False Positives, or Compensating Controls, Noted by ASV for Vulnerability	Page
✓ LOW	0.0	✓ PASS	N/A	N/A	ICMP timestamp response (CVE-1999-0524)	None Noted.	18
✓ LOW	0.0	✓ PASS	161/udp	SNMP	SNMP v2 GetBulk Traffic Amplification	None Noted.	18



## Vulnerabilities Noted for Each IP

<b>62.60.125.113</b>							✓
Severity Level	CVSS Base Score	Compliance Status	Port	Service	Vulnerability Name	Exceptions, False Positives, or Compensating Controls, Noted by ASV for Vulnerability	Page
✓ LOW	0.0	✓ PASS	N/A	N/A	ICMP timestamp response (CVE-1999-0524)	None Noted.	19
✓ LOW	0.0	✓ PASS	161/udp	SNMP	SNMP v2 GetBulk Traffic Amplification	None Noted.	19
<b>194.176.201.49 - No issues Found</b>							✓
<b>194.176.201.53 - No issues Found</b>							✓
<b>194.176.219.225 - No issues Found</b>							✓
<b>194.176.219.226 - No issues Found</b>							✓
<b>194.176.219.227 - No issues Found</b>							✓
<b>194.176.219.241 - No issues Found</b>							✓
<b>194.176.219.242 - No issues Found</b>							✓
<b>194.176.219.243 - No issues Found</b>							✓
<b>194.176.219.244 - No issues Found</b>							✓
<b>194.176.219.245 - No issues Found</b>							✓





## Vulnerabilities Noted for Each IP

### Special Notes:

IP Address	Notes	Item Noted	Scan customers declaration that software is implemented securely (see next column if not implemented securely)	Scan customers description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
62.60.125.97	SNMP Service with potential risk requiring action or explanation on port: 161/udp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Management		
62.60.125.98	SNMP Service with potential risk requiring action or explanation on port: 161/udp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Management		
62.60.125.99	SNMP Service with potential risk requiring action or explanation on port: 161/udp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Management		
62.60.125.113	SNMP Service with potential risk requiring action or explanation on port: 161/udp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Management		



## Vulnerabilities Noted for Each IP

194.176.219.225	ISAKMP Service with potential risk requiring action or explanation on port: 500/udp found.	VPN		
194.176.219.225	unknown Service with potential risk requiring action or explanation on port: 10000/tcp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Administration		
194.176.219.226	ISAKMP Service with potential risk requiring action or explanation on port: 500/udp found.	VPN		
194.176.219.226	unknown Service with potential risk requiring action or explanation on port: 10000/tcp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Administration		
194.176.219.227	ISAKMP Service with potential risk requiring action or explanation on port: 500/udp found.	VPN		
194.176.219.227	unknown Service with potential risk requiring action or explanation on port: 10000/tcp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Administration		
194.176.219.241	ISAKMP Service with potential risk requiring action or explanation on port: 500/udp found.	VPN		
194.176.219.241	unknown Service with potential risk requiring action or explanation on port: 10000/tcp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Administration		
194.176.219.242	ISAKMP Service with potential risk requiring action or explanation on	VPN		



## Vulnerabilities Noted for Each IP

	port: 500/udp found.			
194.176.219.242	unknown Service with potential risk requiring action or explanation on port: 10000/tcp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Administration		
194.176.219.243	ISAKMP Service with potential risk requiring action or explanation on port: 500/udp found.	VPN		
194.176.219.243	unknown Service with potential risk requiring action or explanation on port: 10000/tcp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Administration		
194.176.219.244	ISAKMP Service with potential risk requiring action or explanation on port: 500/udp found.	VPN		
194.176.219.244	unknown Service with potential risk requiring action or explanation on port: 10000/tcp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Administration		
194.176.219.245	ISAKMP Service with potential risk requiring action or explanation on port: 500/udp found.	VPN		
194.176.219.245	unknown Service with potential risk requiring action or explanation on port: 10000/tcp found. Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix D or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	Remote Administration		






## Vulnerabilities Noted for Each IP

Note to Customer: Due to increased risk to the cardholder data environment when the presence of certain software, configurations that may pose a risk to the scan customers environment due to insecure implementation, information disclosure or potential exploit rather than an exploitable vulnerability. Examples of such are:

- Browsing of Directories on Web Servers,
- Remote access such as VPN and SSH,
- Point-of-Sale (POS) Software

For each above special notes in the above table we require documentation of:

- The declared business need for the software,
- A declaration that the software is implemented with strong security controls as well as the details that comprise those controls as per Appendix D of the [PCI ASV Program Guide](#) 
- Any actions taken, including removal, to secure the software as well as the details that comprise those controls.



# Vulnerabilities - Detailed

## Host Compliance Status

**62.60.125.97**

## ICMP timestamp response - (Proven Vulnerable)

Port:	N/A	Compliance Status:	✓ PASS
CVSS Base Score:	0.0 (AV:N/AC:L/AU:N/C:N/I:N/A:N)	Severity Level:	✓ LOW

Exceptions, False Positives, or Compensating Controls. Noted by the ASV for this Vulnerability:  
No additional information provided by the Scan Customer specific to this instance of the Vulnerability.

### Description:

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time -based random number generators in other services. In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

### References:

[CVE-1999-0524](#) [OSVDB:95](#) [XF:icmp-netmask\(306\)](#)   
[XF:icmp-timestamp\(322\)](#)

### Probe Output

Able to determine remote system time.

Solution	Page
The Solution/Recommendation for this issue is located on page:	23

## SNMP v2 GetBulk Traffic Amplification - (Potentially Vulnerable)

Port:	161/udp	Compliance Status:	✓ PASS
CVSS Base Score:	0.0 (AV:N/AC:L/AU:N/C:N/I:N/A:N)	Severity Level:	✓ LOW

Exceptions, False Positives, or Compensating Controls. Noted by the ASV for this Vulnerability:  
No additional information provided by the Scan Customer specific to this instance of the Vulnerability.

### Description:

An SNMP v2 GetBulk operation requests a number of GetNext responses to be returned in a single response. Depending on the MIBs in use, the response can be 6x the size of the request, and because SNMP utilizes UDP, this can be used to conduct traffic amplification attacks against other assets, typically in the form of distributed reflected denial of service (D RDoS) attacks.

### References:

[CERT:TA14-017A](#)

### Probe Output

Running SNMP service

Solution	Page
The Solution/Recommendation for this issue is located on page:	25



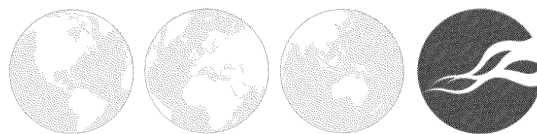
# Vulnerabilities - Detailed

Host Compliance Status	
62.60.125.98	

ICMP timestamp response - (Proven Vulnerable)			
Port:	N/A	Compliance Status:	PASS
CVSS Base Score:	0.0 (AV:N/AC:L/AU:N/C:N/I:N/A:N)	Severity Level:	LOW
Exceptions, False Positives, or Compensating Controls. Noted by the ASV for this Vulnerability: No additional information provided by the Scan Customer specific to this instance of the Vulnerability.			
<b>Description:</b>			
The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time -based random number generators in other services. In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.			
<b>References:</b>			
<a href="#">CVE-1999-0524</a> <a href="#">OSVDB:95</a> <a href="#">XF:icmp-netmask(306)</a> <a href="#">XF:icmp-timestamp(322)</a>			
<b>Probe Output</b>			
Able to determine remote system time.			
<b>Solution</b>			<b>Page</b>
The Solution/Recommendation for this issue is located on page:			23

SNMP v2 GetBulk Traffic Amplification - (Potentially Vulnerable)			
Port:	161/udp	Compliance Status:	PASS
CVSS Base Score:	0.0 (AV:N/AC:L/AU:N/C:N/I:N/A:N)	Severity Level:	LOW
Exceptions, False Positives, or Compensating Controls. Noted by the ASV for this Vulnerability: No additional information provided by the Scan Customer specific to this instance of the Vulnerability.			
<b>Description:</b>			
An SNMP v2 GetBulk operation requests a number of GetNext responses to be returned in a single response. Depending on the MIB s in use, the response can be 6x the size of the request, and because SNMP utilizes UDP, this can be used to conduct traffic amplification attacks against other assets, typically in the form of distributed reflected denial of service (DRDoS) attacks.			
<b>References:</b>			
<a href="#">CERT:TA14-017A</a>			
<b>Probe Output</b>			
Running SNMP service			
<b>Solution</b>			<b>Page</b>
The Solution/Recommendation for this issue is located on page:			25



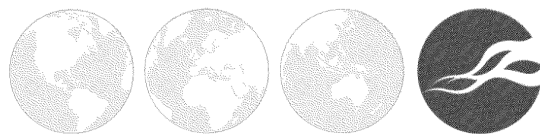


# Vulnerabilities - Detailed

Host Compliance Status	
62.60.125.99	

ICMP timestamp response - (Proven Vulnerable)			
Port:	N/A	Compliance Status:	PASS
CVSS Base Score:	0.0 (AV:N/AC:L/AU:N/C:N/I:N/A:N)	Severity Level:	LOW
Exceptions, False Positives, or Compensating Controls. Noted by the ASV for this Vulnerability: No additional information provided by the Scan Customer specific to this instance of the Vulnerability.			
<b>Description:</b>			
The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time -based random number generators in other services. In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.			
<b>References:</b>			
<a href="#">CVE-1999-0524</a> <a href="#">OSVDB:95</a> <a href="#">XF:icmp-netmask(306)</a> <a href="#">XF:icmp-timestamp(322)</a>			
<b>Probe Output</b>			
Able to determine remote system time.			
<b>Solution</b>			<b>Page</b>
The Solution/Recommendation for this issue is located on page:			23

SNMP v2 GetBulk Traffic Amplification - (Potentially Vulnerable)			
Port:	161/udp	Compliance Status:	PASS
CVSS Base Score:	0.0 (AV:N/AC:L/AU:N/C:N/I:N/A:N)	Severity Level:	LOW
Exceptions, False Positives, or Compensating Controls. Noted by the ASV for this Vulnerability: No additional information provided by the Scan Customer specific to this instance of the Vulnerability.			
<b>Description:</b>			
An SNMP v2 GetBulk operation requests a number of GetNext responses to be returned in a single response. Depending on the MIB s in use, the response can be 6x the size of the request, and because SNMP utilizes UDP, this can be used to conduct traffic amplification attacks against other assets, typically in the form of distributed reflected denial of service (DRDoS) attacks.			
<b>References:</b>			
<a href="#">CERT:TA14-017A</a>			
<b>Probe Output</b>			
Running SNMP service			
<b>Solution</b>			<b>Page</b>
The Solution/Recommendation for this issue is located on page:			25



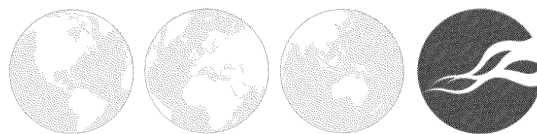
# Vulnerabilities - Detailed

Host Compliance Status	
62.60.125.113	

ICMP timestamp response - (Proven Vulnerable)			
Port:	N/A	Compliance Status:	PASS
CVSS Base Score:	0.0 (AV:N/AC:L/AU:N/C:N/I:N/A:N)	Severity Level:	LOW
Exceptions, False Positives, or Compensating Controls. Noted by the ASV for this Vulnerability: No additional information provided by the Scan Customer specific to this instance of the Vulnerability.			
<b>Description:</b>			
The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time -based random number generators in other services. In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.			
<b>References:</b>			
<a href="#">CVE-1999-0524</a> <a href="#">OSVDB:95</a> <a href="#">XF:icmp-netmask(306)</a> <a href="#">XF:icmp-timestamp(322)</a>			
<b>Probe Output</b>			
Able to determine remote system time.			
<b>Solution</b>			<b>Page</b>
The Solution/Recommendation for this issue is located on page:			23

SNMP v2 GetBulk Traffic Amplification - (Potentially Vulnerable)			
Port:	161/udp	Compliance Status:	PASS
CVSS Base Score:	0.0 (AV:N/AC:L/AU:N/C:N/I:N/A:N)	Severity Level:	LOW
Exceptions, False Positives, or Compensating Controls. Noted by the ASV for this Vulnerability: No additional information provided by the Scan Customer specific to this instance of the Vulnerability.			
<b>Description:</b>			
An SNMP v2 GetBulk operation requests a number of GetNext responses to be returned in a single response. Depending on the MIB s in use, the response can be 6x the size of the request, and because SNMP utilizes UDP, this can be used to conduct traffic amplification attacks against other assets, typically in the form of distributed reflected denial of service (DRDoS) attacks.			
<b>References:</b>			
<a href="#">CERT:TA14-017A</a>			
<b>Probe Output</b>			
Running SNMP service			
<b>Solution</b>			<b>Page</b>
The Solution/Recommendation for this issue is located on page:			25





# Vulnerabilities - Detailed

## Host Compliance Status

**194.176.201.49**



No issues were identified on this host.

## Host Compliance Status

**194.176.201.53**



No issues were identified on this host.

## Host Compliance Status

**194.176.219.225**



No issues were identified on this host.

## Host Compliance Status

**194.176.219.226**



No issues were identified on this host.

## Host Compliance Status

**194.176.219.227**



No issues were identified on this host.

## Host Compliance Status

**194.176.219.241**



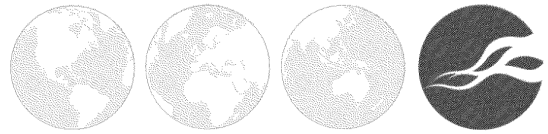
No issues were identified on this host.

## Host Compliance Status

**194.176.219.242**



No issues were identified on this host.



# Vulnerabilities - Detailed

Host Compliance Status	
194.176.219.243	

No issues were identified on this host.

Host Compliance Status	
194.176.219.244	

No issues were identified on this host.

Host Compliance Status	
194.176.219.245	

No issues were identified on this host.

# Vulnerabilities - Solutions



The below solutions are provided to aid resolving vulnerabilities identified in the above report. Please note the severity is rated per the PCI ASV Guidelines CVSSv2 rating system and may not in all cases be the rating applied per host vulnerability when Exceptions, False Positives, or Compensating Controls have been noted by the ASV.

PCI Impact	Solution	Page Number
✓	ICMP timestamp response	23
✓	SNMP v2 GetBulk Traffic Amplification	25

# Vulnerabilities - Solutions



## ICMP timestamp response

CVSS Base Score: 0.0 (AV:N/AC:L/AU:N/C:N/I:N/A:N)

PCI Impact: **PASS**

Severity Level: **LOW**

### Description

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services. In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

### Solution

#### HP-UX

Execute the following command: `ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0` The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

#### Cisco IOS

Use ACLs to block ICMP types 13 and 14. For example: `deny icmp any any 13 deny icmp any any 14` Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench: `permit icmp any any unreachable permit icmp any any echo-reply permit icmp any any time-exceeded permit icmp any any source-quench` The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

#### SGI Irix

IRIX does not offer a way to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using `ipfilterd`, and/or block it at any external firewalls. The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

#### Linux

Linux offers neither a `sysctl` nor a `/proc/sys/net/ipv4` interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using `iptables`, and/or block it at the firewall. For example: `ipchains -A input -p icmp --icmp-type timestamp-request -j DROP ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP` The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Windows NT 4 does not provide a way to block ICMP packets. Therefore, you should block them at the firewall. The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

#### OpenBSD

Set the `"net.inet.icmp.timestampreply"` `sysctl` variable to 0. `sysctl -w net.inet.icmp.timestampreply=0` The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

#### Cisco PIX

A properly configured PIX firewall should never respond to ICMP packets on its external interface. In PIX Software versions 4.1(6) until 5.2.1, ICMP traffic to the PIX's internal interface is permitted; the PIX cannot be configured to NOT respond. Beginning in PIX Software version 5.2.1, ICMP is still permitted on the internal interface by default, but ICMP responses from its internal interfaces can be disabled with the `icmp` command, as follows, where `<inside>` is the name of the internal interface: `icmp deny any 13 <inside> icmp deny any 14 <inside>` Don't forget to save the configuration when you are finished. See Cisco's support document (<http://www.cisco.com/warp/public/110/31.html>) Handling ICMP Pings with the PIX Firewall for more information. The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

#### Sun Solaris

Execute the following commands: `/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp 0 /usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0` The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Use the IPSec filter feature to define and apply an IP filter list that blocks ICMP types 13 and 14. Note that the standard TCP/IP blocking capability under the "Networking and Dialup Connections" control panel is NOT capable of blocking ICMP (only TCP and UDP). The IPSec filter features, while they may seem strictly related to the IPSec standards, will allow you to selectively block these ICMP packets. See



# Vulnerabilities - Solutions



(<http://support.microsoft.com/kb/313190>) for more information. The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

ICMP timestamp responses can be disabled by deselecting the "allow incoming timestamp request" option in the ICMP configuration panel of Windows Firewall. Go to the Network Connections control panel. Right click on the network adapter and select "properties", or select the internet adapter and select File->Properties. Select the "Advanced" tab. In the Windows Firewall box, select "Settings". Select the "General" tab. Enable the firewall by selecting the "on (recommended)" option. Select the "Advanced" tab. In the ICMP box, select "Settings". Deselect (uncheck) the "Allow incoming timestamp request" option. Select "OK" to exit the ICMP Settings dialog and save the settings. Select "OK" to exit the Windows Firewall dialog and save the settings. Select "OK" to exit the internet adapter dialog. For more information, see:  
([http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw\\_understanding\\_firewall.mspx?mfr=true](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true))

Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008

ICMP timestamp responses can be disabled via the netsh command line utility. Go to the Windows Control Panel. Select "Windows Firewall". In the Windows Firewall box, select "Change Settings". Enable the firewall by selecting the "on (recommended)" option. Open a Command Prompt. Enter "netsh firewall set icmpsetting 13 disable" For more information, see:  
([http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw\\_understanding\\_firewall.mspx?mfr=true](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true))

Disable ICMP timestamp replies for the device. If the device does not support this level of configuration, the easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

## References

[CVE-1999-0524](#)

[OSVDB:95](#)

[XF:icmp-netmask\(306\)](#)

[XF:icmp-timestamp\(322\)](#)

## Affected Hosts

[62.60.125.113](#)

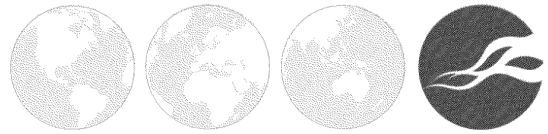
[62.60.125.97](#)

[62.60.125.98](#)

[62.60.125.99](#)



# Vulnerabilities - Solutions



SNMP v2 GetBulk Traffic Amplification			
CVSS Base Score:	<u>0.0 (AV:N/AC:L/AU:N/C:N/I:N/A:N)</u>	PCI Impact:	PASS
		Severity Level:	LOW
Description			
An SNMP v2 GetBulk operation requests a number of GetNext responses to be returned in a single response. Depending on the MIBs in use, the response can be 6x the size of the request, and because SNMP utilizes UDP, this can be used to conduct traffic amplification attacks against other assets, typically in the form of distributed reflected denial of service (DRDoS) attacks.			
Solution			
Restrict access to the SNMP service to only trusted assets			
References			
<u>CERT:TA14-017A</u>			
Affected Hosts			
<u>62.60.125.113</u>	<u>62.60.125.97</u>	<u>62.60.125.98</u>	
<u>62.60.125.99</u>			



# Open Ports List

IP Address	Open Ports
62.60.125.97	161/udp (SNMP)
62.60.125.98	161/udp (SNMP)
62.60.125.99	161/udp (SNMP)
62.60.125.113	161/udp (SNMP)
194.176.201.49	--
194.176.201.53	--
194.176.219.225	500/udp (ISAKMP) 10000/tcp (unknown)
194.176.219.226	500/udp (ISAKMP) 10000/tcp (unknown)
194.176.219.227	500/udp (ISAKMP) 10000/tcp (unknown)
194.176.219.241	500/udp (ISAKMP) 10000/tcp (unknown)
194.176.219.242	500/udp (ISAKMP) 10000/tcp (unknown)
194.176.219.243	500/udp (ISAKMP) 10000/tcp (unknown)
194.176.219.244	500/udp (ISAKMP) 10000/tcp (unknown)
194.176.219.245	500/udp (ISAKMP) 10000/tcp (unknown)

## Additional Information Gathered

IP:Port/Protocol	Vendor	Product	Version	Certainty
No Additional Information Gathered				