				Status	Controls Noted by the ASV for this Vulnerability
Instance: Linux 2 .6	38726 - OpenSSH Username Enumeration Vulnerability (CVE-2018-15473)	Medium	5.0	FAIL	
Instance: Linux 2 .6	82004 - Open UDP Services List	Low	0.0	PASS	This vulnerability is not included in the NVD
Instance: Linux 2 .6	82023 - Open TCP Services List	Low	0.0	PASS	This vulnerability is not included in the NVD
Instance: Linux 2 .6	82003 - ICMP Timestamp Request (CVE-1999-0524)	Low	0.0	PASS	The vulnerability is purely a denial-of-service (DoS) vulnerability

Part 3a-1.2. Consolidated Solution/Correction Plan for the above IP Address:

For Linux 2.6

These vulnerabilities can be resolved by performing the following 4 steps.

Vulnerability	Remediation Step
OpenSSH Username Enumeration Vulnerability	Customers are advised to upgrade to OpenSSH 7.8 or later versions to remediate this vulnerability. Patch: Following are links for downloading patches to fix the vulnerabilities: OpenSSH 7.8 or later
Open UDP Services List	Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.
Open TCP Services List	Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.
ICMP Timestamp Request	You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the *Ping of Death* or *Smurf* attacks. However, you should never filter **ALL** ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks. It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

Part 3b. Special Notes by Component

Part 3b-1.

Component	Special Note	Item Noted	Scan Customer's description of action taken and declaration that software is either implemented securely or removed
147.75.xxx.xx	Remote Access	Remote Access Service name: SSH on TCP port 22.	
147.75.xxx.x Protocol: tcp Port: 22	Remote Access	Remote Access ssh SSH Remote Login Protocol ssh	

Part 3c. Special Notes - Full Text

Remote Access
Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, 1) justify the business need for this software to the ASV and confirm it is implemented securely, or 2) confirm it is disabled/removed. Consult your ASV if you have questions about this Special Note.

Part 4a. Scan Scope Submitted by Scan Customer for discovery

Part 4b. Scan Customer Designated "In- Scope" Components (Scanned)

Part 4c. Scan Customer Designated "Out-Of-Scope" components (Not Scanned)