
LGMS
CONFIDENTIAL
PCI ASV Scanning Report
Bank Simpanan Nasional
REF NO: BSN-MY-SPA-R1-2020
REV NO: 1.0

3.11. 211.25.204.15

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
211.25.204.15 protocol: tcp port: 443	CVE-2011-3389, TLS/SSL Server is enabling the BEAST attack	medium	4.3	FAIL	
211.25.204.15 protocol: tcp port: 443	Undefined CVE, TLS Server Supports TLS version 1.0	medium	4.3	FAIL	Support for SSL and early TLS is a violation of the PCI DSS, and result in an automatic failure.
211.25.204.15 protocol: tcp port: 443	CVE-2013-0169, TLS/SSL Timing Side-Channel Attacks, aka the "Lucky Thirteen" Attack	low	2.6	PASS	
211.25.204.15 protocol: tcp port: 443	Undefined CVE, TLS/SSL Server Supports The Use of Static Key Ciphers	low	2.6	PASS	
211.25.204.15 protocol: tcp port: 443	Undefined CVE, TLS Server Supports TLS version 1.1	low	2.6	PASS	
211.25.204.15 protocol: tcp port: 443 instance: HTTPS	Undefined CVE, A running service was discovered	low	0.0	PASS	
211.25.204.15	Undefined CVE, TCP timestamp response	low	0.0	PASS	

3.12. Consolidated Solution/Correction Plan for the above Component:

3.12.1. For HTTPS

These vulnerabilities can be resolved by performing the following 4 steps. The total estimated time to perform all of these steps is 4 hours.

Remediation Step	Estimated Time
Disable insecure TLS/SSL protocol support	1 hour
Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled	1 hour
Disable TLS/SSL support for static key cipher suites	1 hour
Disable TLS/SSL support for CBC cipher suites or patch the cipher suite library	1 hour

3.12.2. Further Investigation Required

LGMS could not determine the software running on the target system. The following solutions apply to a variety of software. Choose the one that applies to your system type.

For Linux

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.

Remediation Step	Estimated Time
Disable TCP timestamp responses on Linux	5 minutes

For 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, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 R2, Standard Edition, Microsoft Windows Server 2008 R2, Enterprise Edition, Microsoft Windows Server 2008 R2, Datacenter Edition, Microsoft Windows Server 2008 R2, Web Edition, Microsoft Windows Server 2012, Microsoft Windows Server 2012 Standard Edition, Microsoft Windows Server 2012 Foundation Edition, Microsoft Windows Server 2012 Essentials Edition, Microsoft Windows Server 2012 Datacenter Edition, Microsoft Windows Storage Server 2012, 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 7, Microsoft Windows 7 Home, Basic Edition, Microsoft Windows 7 Home, Basic N Edition, Microsoft Windows 7 Home, Premium Edition, Microsoft Windows 7 Home, Premium N Edition, Microsoft Windows 7 Ultimate Edition, Microsoft Windows 7 Ultimate N Edition, Microsoft Windows 7 Enterprise Edition, Microsoft Windows 7 Enterprise N Edition, Microsoft Windows 7 Professional Edition, Microsoft Windows 7 Starter Edition, Microsoft Windows 7 Starter N Edition, Microsoft Windows 8, Microsoft Windows 8 Enterprise Edition, Microsoft Windows 8 Professional Edition, Microsoft Windows 8 RT, Microsoft Windows Longhorn Server Beta

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.

Remediation Step	Estimated Time
Disable TCP timestamp responses on Windows versions since Vista	5 minutes

For FreeBSD

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.

Remediation Step	Estimated Time
Disable TCP timestamp responses on FreeBSD	5 minutes

For Cisco

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.

Remediation Step	Estimated Time
Disable TCP timestamp responses on Cisco	5 minutes

For OpenBSD

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.

Remediation Step	Estimated Time
Disable TCP timestamp responses on OpenBSD	5 minutes

For 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, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows 98SE, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server, Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows XP Tablet PC Edition, Microsoft Windows CE, 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, Microsoft Windows Server 2003 R2, Microsoft Windows Server 2003 R2, Standard Edition, Microsoft Windows Server 2003 R2, Enterprise Edition, Microsoft Windows Server 2003 R2, Datacenter Edition, Microsoft Windows Server 2003 R2, Web Edition, Microsoft Windows Small Business Server 2003 R2, Microsoft Windows Server 2003 R2, Express Edition, Microsoft Windows Server 2003 R2, Workgroup Edition

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.

Remediation Step	Estimated Time
Disable TCP timestamp responses on Windows versions before Vista	5 minutes

3.19. 58.27.45.172

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
58.27.45.172 protocol: tcp port: 443	CVE-2019-11358, jQuery Vulnerability: CVE-2019-11358	medium	4.3	FAIL	
58.27.45.172 protocol: tcp port: 443	CVE-2011-3389, TLS/SSL Server is enabling the BEAST attack	medium	4.3	FAIL	
58.27.45.172 protocol: tcp port: 443	Undefined CVE, TLS Server Supports TLS version 1.0	medium	4.3	FAIL	Support for SSL and early TLS is a violation of the PCI DSS, and result in an automatic failure.
58.27.45.172 protocol: tcp port: 443	CVE-2013-0169, TLS/SSL Timing Side-Channel Attacks, aka the "Lucky Thirteen" Attack	low	2.6	PASS	
58.27.45.172 protocol: tcp port: 443	Undefined CVE, TLS/SSL Server Supports The Use of Static Key Ciphers	low	2.6	PASS	
58.27.45.172 protocol: tcp port: 443	Undefined CVE, TLS Server Supports TLS version 1.1	low	2.6	PASS	
58.27.45.172 protocol: tcp port: 443 instance: HTTPS	Undefined CVE, A running service was discovered	low	0.0	PASS	
58.27.45.172	Undefined CVE, TCP timestamp response	low	0.0	PASS	

3.20. Consolidated Solution/Correction Plan for the above Component:

3.20.1. For HTTPS

These vulnerabilities can be resolved by performing the following 4 steps. The total estimated time to perform all of these steps is 4 hours.

Remediation Step	Estimated Time
Disable insecure TLS/SSL protocol support	1 hour
Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled	1 hour
Disable TLS/SSL support for static key cipher suites	1 hour
Disable TLS/SSL support for CBC cipher suites or patch the cipher suite library	1 hour

3.20.2. Further Investigation Required

LGMS could not determine the software running on the target system. The following solutions apply to a variety of software. Choose the one that applies to your system type.

For < 3.4.0

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 1 hour.

Remediation Step	Estimated Time
Upgrade to jQuery version 3.4.0	1 hour

For Cisco

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.

Remediation Step	Estimated Time
Disable TCP timestamp responses on Cisco	5 minutes

For FreeBSD

These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.

Remediation Step	Estimated Time
Disable TCP timestamp responses on FreeBSD	5 minutes

For 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, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 R2, Standard Edition, Microsoft Windows Server 2008 R2,

Enterprise Edition, Microsoft Windows Server 2008 R2, Datacenter Edition, Microsoft Windows Server 2008 R2, Web Edition, Microsoft Windows Server 2012, Microsoft Windows Server 2012 Standard Edition, Microsoft Windows Server 2012 Foundation Edition, Microsoft Windows Server 2012 Essentials Edition, Microsoft Windows Server 2012 Datacenter Edition, Microsoft Windows Storage Server 2012, 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 7, Microsoft Windows 7 Home, Basic Edition, Microsoft Windows 7 Home, Basic N Edition, Microsoft Windows 7 Home, Premium Edition, Microsoft Windows 7 Home, Premium N Edition, Microsoft Windows 7 Ultimate Edition, Microsoft Windows 7 Ultimate N Edition, Microsoft Windows 7 Enterprise Edition, Microsoft Windows 7 Enterprise N Edition, Microsoft Windows 7 Professional Edition, Microsoft Windows 7 Starter Edition, Microsoft Windows 7 Starter N Edition, Microsoft Windows 8, Microsoft Windows 8 Enterprise Edition, Microsoft Windows 8 Professional Edition, Microsoft Windows 8 RT, Microsoft Windows Longhorn Server Beta
These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.

Remediation Step	Estimated Time
Disable TCP timestamp responses on Windows versions since Vista	5 minutes

For Linux
These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.

Remediation Step	Estimated Time
Disable TCP timestamp responses on Linux	5 minutes

For OpenBSD
These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.

Remediation Step	Estimated Time
Disable TCP timestamp responses on OpenBSD	5 minutes

For 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, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows 98SE, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server, Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows XP Tablet PC Edition, Microsoft Windows CE, 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, Microsoft Windows Server 2003 R2, Microsoft Windows Server 2003 R2, Standard Edition, Microsoft Windows Server 2003 R2, Enterprise Edition, Microsoft Windows Server 2003 R2, Datacenter Edition, Microsoft Windows Server 2003 R2, Web Edition, Microsoft Windows Small Business Server 2003 R2, Microsoft Windows Server 2003 R2, Express Edition, Microsoft Windows Server 2003 R2, Workgroup Edition
These vulnerabilities can be resolved with a single step. The estimated time to perform this step is 5 minutes.