Company B Vulnerability Report

Company B performed this vulnerability assessment in anticipation of system integration with Company A. This assessment was performed by a qualified third-party assessor, and this report has been generated with the results. This assessment was performed in accordance with a methodology described in NIST 800-30 Rev 1 to identify the following:

- Vulnerabilities using the CVSS model
- Severity
- Likelihood of occurrence

Table A. Risk Classifications

Risk Level	Description
High	The loss of confidentiality, integrity, or availability may be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The loss of confidentiality, integrity, or availability may be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Low	The loss of confidentiality, integrity, or availability may be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Table B. Severity

Severity Level (CVSS Model)	Description
Critical	• Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices. • Exploitation is usually straightforward in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims and does not need to persuade a target user, for example, via social engineering, to perform any special functions.
High	• The vulnerability is difficult to exploit. • Exploitation could result in elevated privileges. • Exploitation could result in significant data loss or downtime.
Medium	• Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. • Denial of service vulnerabilities that are difficult to set up. • Exploits that require an attacker to reside on the same local network as the victim.

	• Vulnerabilities where exploitation provides only very limited access. • Vulnerabilities that require user privileges for successful exploitation.
Low	Exploitation of such vulnerabilities usually requires local or physical system access and would have little impact on the organization.

Table C. Level of Effort

Level of Effort	**Description**
High	This requires a high level of dedicated effort from one or more teams on critical systems, including patching, multiple configuration changes, or highly technical changes that risk bringing services down.
Moderate	This is a medium-level effort that requires substantial dedication from a partial or entire team. This could impact services or cause a partial outage.
Low	These are individual or small team efforts generally requiring a minimal time commitment and require running an update or remedial command or series of commands that will not impact production services.

Table D. System Inventory

System Components	
Servers	Virtualized farm running on Hyper-V (2 hosts). Windows Server 2019 and Ubuntu Linux. Approximately 20 virtualized servers (across the 2 hosts), including the following roles: • (Ubuntu Linux) FTP server for EDI Incoming Operations • 3x Domain Controllers (1 used for M365 identity sync) • 1x File Storage/Server • 1x Ruby On Rails server • 3x ElasticSearch servers (cluster) • 5x web application servers (Ubuntu Linux cluster, 1x PostGRESQL, 1x MariaDB SQL, 3x running nginX Plus w\reverse caching proxy, 1x running Apache Tomcat, PHP 8, hosting SSL/TLS certificates) • 4x Remote Desktop Servers for internal shared/applications • 2x legacy Exchange servers (post-migration)
75 Workstations	Windows XP, 7, 10/11 Pro, Ubuntu Linux, MacOS
Switches	HPE JL262A Aruba 2930F 48G PoE+
Firewall	2x Sophos XG firewalls
Border router	Verizon FIOS router (CR1000A)
Laptops	Windows 10, 11, Ubuntu 22.04 LTS, MacOS (Ventura, Monterey, Big Sur)

Wireless Access Points	10x HPE JZ337A Aruba AP-535
Cable plant	Cat6a

Table E. Risk Identification

Risk #	Vulnerability (NVT Name)	NVT OID	Severity	Risk	Level of Effort
1	Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	1.3.6.1.4.1.25623.1.0.108010	Critical	High	High
2	MFA not enforced across all users		High	High	High
3	Rexec service is running	1.3.6.1.4.1.25623.1.0.100111	High	High	Low
4	All users have local administrative privileges		Medium	Moderate	High
5	Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability on publicly-facing server	1.3.6.1.4.1.25623.1.0.140051	Critical	High	Moderate
6	Operating System (OS) End of Life (EOL) Detection	1.3.6.1.4.1.25623.1.0.103674	Critical	High	Low
7	rlogin Passwordless Login	1.3.6.1.4.1.25623.1.0.113766	High	Moderate	Low
8	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	1.3.6.1.4.1.25623.1.0.143545	Critical	High	Moderate
9	PostgreSQL weak password	1.3.6.1.4.1.25623.1.0.103552	High	High	Low

10	PostgreSQL admin is reachable from internet		Critical	High	Low
11	VNC Brute Force Login	1.3.6.1.4.1.25623.1.0.106056	High	High	Low
12	FTP Brute Force Logins Reporting	1.3.6.1.4.1.25623.1.0.108718	High	High	Low
13	phpinfo() output Reporting	1.3.6.1.4.1.25623.1.0.11229	High	Moderate	Low
14	vsftpd Compromised Source Packages Backdoor Vulnerability	1.3.6.1.4.1.25623.1.0.103185	High	High	Moderate
15	rsh Unencrypted Cleartext Login	1.3.6.1.4.1.25623.1.0.100080	High	Moderate	Moderate
16	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	1.3.6.1.4.1.25623.1.0.105042	High	Moderate	Moderate
17	Anonymous FTP Login Reporting	1.3.6.1.4.1.25623.1.0.900600	Moderate		Low
18	Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check	1.3.6.1.4.1.25623.1.0.108011	High	Moderate	High
19	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	1.3.6.1.4.1.25623.1.0.111012	Moderate	Moderate	Moderate
20	Weak Host Key Algorithm(s) (SSH)	1.3.6.1.4.1.25623.1.0.117687	Moderate	Moderate	Moderate

Company B Cyber Security Tools

Company B has provided this list of cyber security tools in anticipation of being acquired by Company A. This list is assumed to be complete.

Table A. Cyber Security Tools

Tool Name	Purpose
Sophos/Intercept X	Endpoint Detection and Response
OneTrust	Data privacy/Data lifecycle management
Code42	Data-centric security
Sophos XG	Next-Gen Firewalls
No tool available	Mobile Device & Application Management
DUO	Identity and Access Management
Akamai	Application Security
Mimecast	Messaging Security
Arctic Wolf	Managed Security Services Provider
Cisco Umbrella	DNS Security
In progress	Cyber security policy
In progress	Written Information Security Policy (WISP)
In progress	Written procedures
Minimal	Documentation of environment