SUMERU SOFTWARE SOLUTIONS (P) LTD.

Network Vulnerability Assessment Report

for

Bajaj Auto

Sumeru Software Solutions (P) Ltd.

1st Floor "Samvit" Building
Udayapura,Bangalore - 560 082
Karnataka, India
www.sumeru.com

Disclaimer

This document has been prepared by Sumeru's Information Security team for the consideration of **Bajaj Auto**, Here-in referred as **BA**.

Whilst all due care and diligence has been taken in the preparation of this document it is not impossible that a document of this nature may contain errors or omissions as a result of a misunderstanding of Clients' requirements. In particular, any recommendations are made in good faith as guidelines to assist the client in evaluation and must not be constructed as warranties of any kind. Findings in this report are based on various tests conducted using third party tools and Sumeru has put its best efforts to eliminate all the false positives reported by these tools.

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. Sumeru cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Table of Contents

1. Introduction & Objective

Client: Bajaj Auto.

Vendor: Sumeru Software Solutions (P) Ltd., Information Security specialists, based in Bangalore, India here-in referred as Sumeru.

BA had appointed Sumeru to assess the security posture of its critical infrastructure (as mentioned in scope). To achieve this Sumeru conducted a Vulnerability Assessment & Penetration Testing for External/Internal network/systems.

Objective

The objective of this assignment was to identify any single or chained vulnerabilities that exists on these systems within a limited time frame and to recommend appropriate measures to mitigate the identified vulnerabilities.

Efforts were focused on the identification and exploitation of security weaknesses that could allow an internal & external attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general internal & external user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP800-115, PTES, OSSTMM v3 and Penetration Testing Guidance given by PCI Security Standards Council with all tests and actions being conducted under contained & controlled condition.

2. Project Timeline

Title	Network Vulnerability Assessment Report		
Version	1.0	Remarks	
Client Name	Bajaj Auto		
Project Name	Bajaj Auto - Network Vulnerability Assessment		
Type of Assessment	Internal / External Testing	Black Box	
Pen Tester	Swetha M	Information Security Engineer	
Reviewer	Rajesh D	Information Security Engineer	
Technical Contact	infosec@sumerusolutions.com		

3. Scope

BA has provided below IP addresses to be covered as a part of the scope, the tables below shows the affected IPs with **CRITICAL**, **HIGH**, **MEDIUM** and **LOW** vulnerabilities.

System wise Number of Vulnerabilities Reported

External Systems						
S/N	Hostname	IP Addresses	Risk Level			
			CRITICAL	HIGH	MEDIUM	LOW
1	Endpoint	104.211.102.2	0	0	0	0
2	Endpoint	104.211.93.166	0	0	0	0
3	Endpoint	104.211.98.34	0	0	2	2
4	Endpoint	104.211.99.99	0	0	2	4
5	Endpoint	13.71.18.246	0	0	0	1
6	Endpoint	13.71.19.216	0	0	0	0
7	Endpoint	40.65.188.45	0	0	0	0
8	Endpoint	52.172.152.28	0	0	0	0
9	Endpoint	52.172.154.92	0	0	0	0
10	Endpoint	52.172.158.101	0	0	0	0
11	Endpoint	52.172.194.178	0	0	0	3
12	Endpoint	52.172.218.153	0	0	1	3
13	Endpoint	40.65.188.228	0	0	0	0
14	Endpoint	40.65.188.230	0	0	0	0
15	Endpoint	40.65.188.232	0	0	0	0
16	Endpoint	40.65.188.235	0	0	0	0
17	Endpoint	40.65.188.239	0	0	0	0
18	Endpoint	40.65.188.197	0	0	0	0
19	Endpoint	13.71.18.200	0	0	0	0
20	Endpoint	13.71.18.202	0	0	0	0
21	Endpoint	13.71.18.204	0	0	0	0
22	Endpoint	13.71.18.205	0	0	0	0
23	Endpoint	13.71.18.224	0	0	0	0
24	Endpoint	13.71.18.239	0	0	0	0
25	Endpoint	13.71.18.241	0	0	0	0
Total			**0**	**0**	**5**	**13**

Internal Systems						
S/N	Hostname	IP Addresses	Risk Level			
			CRITICAL	HIGH	MEDIUM	LOW
1	eHTTP 2.0	10.20.2.5	0	0	0	2
2	BMC Software (Apache httpd)	10.20.2.105	0	0	0	2
3	Apache httpd	10.20.2.108	0	0	0	4

4	Login.. (Microsoft IIS httpd 8.5)	10.20.2.124	0	0	0	2
5	Telephone Directory (Microsoft IIS httpd 8.5)	10.20.2.158	0	0	0	1
6	VMware ESX 4.0 Server httpd	10.12.104.10	0	0	0	0
7	VMware ESX 4.0 Server httpd	10.12.104.12	0	0	0	0
8	Rockwell Automation (GoAhead WebServer)	10.12.104.242	0	0	0	0
9	Rockwell Automation (GoAhead-Webs)	10.12.104.243	0	0	0	0
10	Infrastructure Management (Apache httpd)	10.20.2.156	0	0	1	4
11	AKNEWBMS01 - ProCurve Switch 2610-24 (J9085A) (eHTTP 2.0)	10.11.0.30	0	0	0	0
12	Dell PowerVault TL4000 http config	10.20.2.73	0	0	0	0
13	Dell PowerVault TL4000 http config	10.20.2.222	0	0	0	0
14	Dell PowerVault TL4000 http config	10.20.2.153	0	0	0	0
15	Cisco IOS http config	10.20.2.106	0	0	0	0
16	QNAP HS-210 or TS-219P NAS http config 1.0	10.11.0.22	0	0	0	2
17	thttpd 2.25b 29dec2003	10.12.104.32	0	0	0	0
18	HP Storage Management Utility	10.12.104.35	0	0	0	3
19	Microsoft SQL Server 11.0.2218.0	10.12.104.58	0	0	1	3
20	Microsoft SQL Server 11.0.6020.0	10.20.2.202	0	0	1	1
21	BAL-LCS	10.20.2.102	0	0	0	2
22	10.20.2.103	10.20.2.103	0	0	0	0
23	balemsaddmapp.bajajauto.co.in	10.20.2.105	0	0	0	0
24	BALEMSENTIAPP	10.20.2.108	0	0	0	0
25	10.20.2.109	10.20.2.109	0	0	0	0
26	BALEMSBBCAAPP	10.20.2.110	0	0	0	1
27	BALAKPERFEXAPP	10.20.2.111	0	0	0	3
28	BALANALYTICSAPP	10.20.2.112	0	0	0	1
29	BALAKACSAPP	10.20.2.113	0	0	0	4
30	BALQVTest02	10.20.2.114	0	0	0	0
31	BALQVPUBNODE	10.20.2.117	0	0	0	1
32	BALAKSSR	10.20.2.118	0	0	0	1
33	BALAKACAD02	10.20.2.12	0	0	0	1
34	BALQVNPRINT	10.20.2.120	0	0	0	1
35	BALAKVCENTER6	10.20.2.121	0	0	1	0
36	TISDVAPP	10.20.2.122	0	0	1	4
37	BALCOMMONDB	10.20.2.123	0	0	0	1

38	BALAKSUMMDB01	10.20.2.124	0	0	0	0
39	BALAKSCRUM	10.20.2.125	0	0	0	1
40	BALAKFIXIT	10.20.2.126	0	0	0	1
41	BALAKGEARBOX	10.20.2.128	0	0	0	2
42	BALAKLMS	10.20.2.133	0	0	0	3
43	10.20.2.136	10.20.2.136	0	0	0	0
44	BALMSBIAPP	10.20.2.137	0	0	0	1
45	10.20.2.138	10.20.2.138	0	0	0	0
46	10.20.2.143	10.20.2.143	0	0	0	0
47	BALAKPMPAPP01	10.20.2.148	0	0	0	1
48	BALAKSSR02	10.20.2.150	0	0	0	1
49	BALQVTEST	10.20.2.151	0	0	0	1
50	Linux	10.20.2.152	0	1	1	2
51	BALAKWEIGMC	10.20.2.154	0	0	0	1
52	BALBTOM01	10.20.2.155	0	0	1	2
53	BALBTOM02	10.20.2.156	0	0	0	0
54	BALBTOM03	10.20.2.157	0	0	0	1
55	BALAKTELDIRAPP	10.20.2.158	0	0	0	0
56	balecms.bajajauto.co.in	10.20.2.161	0	1	1	5
57	BALTESTSQLDB2	10.20.2.162	0	0	0	2
58	BALAKDC01	10.20.2.164	0	0	0	1
59	BALAKECUDB	10.20.2.165	0	0	0	1
60	BALAKDP	10.20.2.168	0	0	0	1
61	balticldev.bajajauto.co.in	10.20.2.169	0	0	0	1
62	Linux	10.20.2.178	0	0	0	0
63	BALAKQLIKPOC01	10.20.2.179	0	0	0	1
64	BALAKNAS01	10.20.2.180	0	0	0	1
65	10.20.2.188	10.20.2.188	0	0	0	0
66	BAJAJ-AV	10.20.2.19	0	0	0	1
67	SYMTRAX_POC	10.20.2.202	0	0	0	0
68	BALTISDEV	10.20.2.203	0	0	0	1
69	10.20.2.206	10.20.2.206	0	0	0	0
70	BALAKRMS01	10.20.2.215	0	0	0	1
71	BALQVPROD	10.20.2.216	0	0	0	1
72	BALQVPUB	10.20.2.217	0	0	0	1
73	BALAKBOT01	10.20.2.224	0	0	0	2
74	BALAKPENAS01	10.20.2.226	0	0	0	1
75	BALAKNMS	10.20.2.238	0	0	0	2
76	BALSELFHELP	10.20.2.24	0	0	0	1
77	BALAKCHPUNCH	10.20.2.246	0	0	0	1
78	BALAKDHCP	10.20.2.25	0	0	0	1
79	BALAKBlackBox01.bajajauto.co.in	10.20.2.26	0	0	0	1

80	10.20.2.27	10.20.2.27	0	0	0	0
81	BALAKDCEXCH02	10.20.2.28	0	0	0	1
82	BALAKCAS02	10.20.2.30	0	0	0	1
83	balakeg01.bajajauto.co.in	10.20.2.32	0	0	0	0
84	balakeg02.bajajauto.co.in	10.20.2.33	0	0	0	0
85	BALAKSIEMSORM01	10.20.2.37	0	0	0	2
86	balaksmokesc01.bajajauto.co.in	10.20.2.39	0	0	0	0
87	BALAKDC03	10.20.2.41	0	0	0	1
88	BALAKDC04	10.20.2.42	0	0	0	1
89	balakhts01.bajajauto.co.in	10.20.2.43	0	0	0	1
90	fepool.bajajauto.co.in	10.20.2.49	0	0	0	0
91	BALAKFE02	10.20.2.50	0	0	0	1
92	BALAKADFS01	10.20.2.52	0	0	0	1
93	balakadfs02.bajajauto.co.in	10.20.2.54	0	0	0	1
94	10.20.2.59	10.20.2.59	0	0	0	0
95	BALAKWSUS01	10.20.2.60	0	0	0	1
96	BALAK-NEWVMS	10.20.2.61	0	0	0	2
97	Windows	10.20.2.62	0	0	0	1
98	BALAKDMS01	10.20.2.72	0	0	0	1
99	10.20.2.78	10.20.2.78	0	0	0	0
100	BALAKHPCONCTPOC	10.20.2.79	0	0	0	1
101	BALTALLY	10.20.2.81	0	0	0	1
102	BALGARTNERDOCS	10.20.2.82	0	0	0	1
103	balenpaxapp	10.20.2.83	0	0	0	4
104	BALAKBKS02	10.20.2.84	0	0	0	1
105	balvendattdb	10.20.2.85	0	0	0	1
106	BALVENDATTAPP	10.20.2.86	0	0	0	4
107	zabbix.bajajauto.co.in	10.20.2.87	0	0	0	4
108	balakcctv02.bajajauto.co.in	10.20.2.88	0	0	0	0
109	BALAKSEPM03	10.20.2.90	0	0	0	1
110	BALAKASC	10.20.2.91	0	0	0	1
111	BALAKACS	10.20.2.92	0	0	0	1
112	10.20.2.94	10.20.2.94	0	0	0	0
113	BALATTAPP16	10.20.2.95	0	0	0	4
114	BALATTDB16	10.20.2.96	0	0	0	1
115	BALAKSUMMAPP	10.20.2.97	0	0	0	1
116	BALAKSUMMDB	10.20.2.98	0	0	0	1
117	BALAKIAMSAPP	10.20.2.228	0	0	0	4
118	BALMOBBILLMGR	10.20.2.229	0	0	1	1
119	BALIMCPROD	10.20.2.23	0	0	0	2
120	BALAKPERFEXDB	10.20.2.233	0	0	0	1
121	BALAKPFAPP01	10.20.2.234	0	0	0	3
122	BALAKPFDB01	10.20.2.235	0	0	0	1

123	BALAKEHSSOFT	10.20.2.236	0	0	0	1
124	ak-pcs-0192-ls.bajajauto.co.in	10.11.0.12	0	0	0	3
125	10.11.130.153	10.11.130.153	0	0	0	0
126	balwjdrvcenter.bajajauto.co.in	10.12.104.25	0	0	1	1
127	balwjeoldev01.bajajauto.co.in	10.12.104.252	0	0	0	1
128	balwjscrum.bajajauto.co.in	10.12.104.253	0	0	0	1
129	balwjweigmc.bajajauto.co.in	10.12.104.254	0	0	1	4
130	balwjdcvcenter.bajajauto.co.in	10.12.104.26	0	0	1	1
131	wl-pcs-0900.bajajauto.co.in	10.12.104.33	0	0	1	1
132	balwjbkp01.bajajauto.co.in	10.12.104.42	0	0	0	1
133	balwjsapprint.bajajauto.co.in	10.12.104.46	0	0	0	1
134	balwjbstdb.bajajauto.co.in	10.12.104.51	0	0	1	1
135	balwjshtl-test.bajajauto.co.in	10.12.104.55	0	0	0	1
136	balwjshtlprod01.bajajauto.co.in	10.12.104.56	0	0	0	1
137	balwjdhcp01.bajajauto.co.in	10.12.104.57	0	0	0	1
138	balwjsepm01.bajajauto.co.in	10.12.2.18	0	0	0	1
139	balwjhyperv01.bajajauto.co.in	10.12.2.249	0	0	0	1
140	balwjwsus03.bajajauto.co.in	10.12.2.250	0	0	0	1
141	balwjwsus02.bajajauto.co.in	10.12.2.28	0	0	0	1
142	wl-pcs-0274-ls.bajajauto.co.in	10.12.2.36	0	0	0	2
143	balckmes01.bajajauto.co.in	10.13.14.33	0	0	0	1
144	balckmes02.bajajauto.co.in	10.13.14.34	0	0	0	1
145	balckbkp01.bajajauto.co.in	10.13.14.36	0	0	0	1
146	balckecudb.bajajauto.co.in	10.13.14.62	0	0	0	1
147	balckhyper-v.bajajauto.co.in	10.13.14.63	0	0	0	1
148	balckwsus03.bajajauto.co.in	10.13.14.64	0	0	0	1
149	balcksepm01.bajajauto.co.in	10.13.14.65	0	0	0	0
150	10.20.127.10	10.20.127.10	0	0	0	0
151	10.20.127.4	10.20.127.4	0	0	0	0
152	10.20.127.5	10.20.127.5	0	0	0	0
153	10.20.127.6	10.20.127.6	0	0	0	0
154	10.20.127.7	10.20.127.7	0	0	0	0
155	10.20.127.8	10.20.127.8	0	0	0	0
156	10.20.127.9	10.20.127.9	0	0	0	0
157	drrdp.bajajauto.co.in	10.20.32.34	0	0	0	1
158	baldrdc01.bajajauto.co.in	10.20.32.36	0	0	0	1
159	balakdrexch02.bajajauto.co.in	10.20.32.40	0	0	0	3
160	baldrcas02.bajajauto.co.in	10.20.32.41	0	0	0	1
161	10.20.7.35	10.20.7.35	0	0	0	0
162	Linux	10.20.7.44	0	0	0	1
163	10.20.7.50	10.20.7.50	0	0	0	1
164	balptsepm01.bajajauto.co.in	10.22.0.119	0	0	0	1
165	balpthyperv01.bajajauto.co.in	10.22.0.32	0	0	0	1

166	balptwsus03.bajajauto.co.in	10.22.0.34	0	0	0	1
167	balptwsus02.bajajauto.co.in	10.22.1.29	0	0	0	1
168	pt-srv-0004.bajajauto.co.in	10.22.1.6	0	0	0	1
169	baldgdpapp.bajajauto.co.in	172.16.1.103	0	0	0	1
170	baldgwbfsp01.bajajauto.co.in	172.16.1.140	0	0	1	3
171	baldgktmapp.bajajauto.co.in	172.16.1.141	0	0	0	1
172	balwebsvr01.bajajauto.co.in	172.16.1.34	0	0	0	2
173	sepmdg.bajajauto.co.in	172.16.1.42	0	0	0	1
174	baldgdc03.bajajauto.co.in	172.16.1.45	0	0	0	1
175	baldgtms.bajajauto.co.in	172.16.1.46	0	0	0	1
176	baldgdb01.bajajauto.co.in	172.16.1.47	0	0	0	1
177	Linux	172.16.1.48	0	0	0	0
178	Linux	10.20.10.60	0	0	0	0
179	Linux	10.20.10.58	0	0	0	0
180	Linux	10.20.10.59	0	0	0	0
181	Linux	10.20.10.48	0	0	0	0
182	Linux	10.20.10.53	0	0	0	0
183	Linux	10.20.10.54	0	0	0	0
184	Linux	10.20.10.55	0	0	0	0
185	Linux	10.20.10.56	0	0	0	0
186	Linux	10.20.10.57	0	0	0	0
187	Linux	10.20.10.51	0	0	0	2
188	Linux	10.20.10.33	0	0	0	2
189	Linux	10.20.10.50	0	0	0	0
190	Linux	10.20.10.42	0	0	0	0
191	Linux	10.20.10.62	0	0	0	0
192	vhbaltst01ap01.dc.hec.bajajauto.co.in	10.20.10.61	0	0	0	0
193	Linux	10.20.10.66	0	0	0	0
194	Linux	10.20.10.65	0	0	0	0
195	Linux	10.20.10.64	0	0	0	0
196	HP JetDirect	10.20.10.36	0	0	0	0
197	HP JetDirect	10.20.10.35	0	0	0	0
198	Linux	10.20.10.34	0	0	0	0
199	Linux	10.20.10.45	0	0	0	0
200	Linux	10.20.10.43	0	0	0	0
201	Linux	10.20.10.44	0	0	0	0
202	Linux	10.20.10.46	0	0	0	0
203	Linux	10.20.10.74	0	0	0	0
204	Linux	10.20.10.75	0	0	0	0
205	Linux	10.20.10.73	0	0	0	0
206	Linux	10.20.10.76	0	0	0	0
207	Linux	10.20.10.49	0	0	0	0

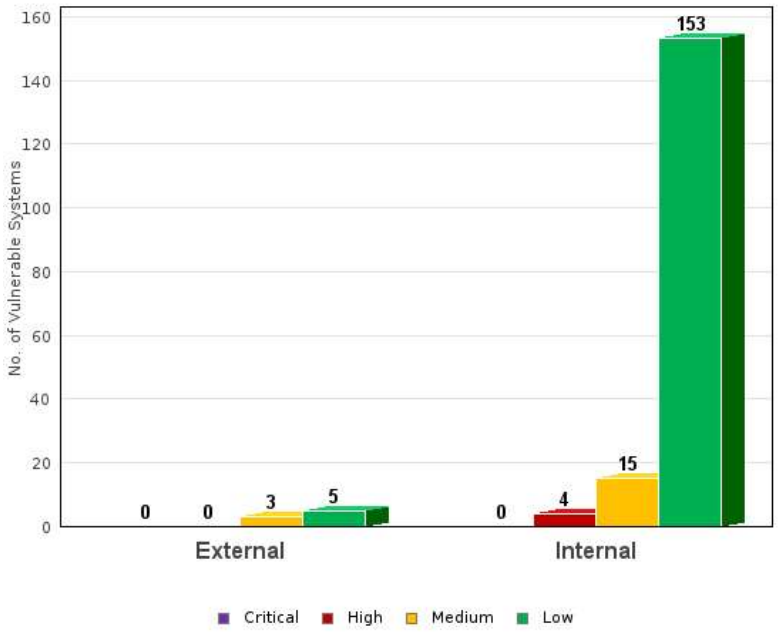
208	solmanprd.bajajauto.co.in	10.20.10.29	0	0	0	0
209	hccsrv.bajajauto.co.in	10.20.10.63	0	0	0	0
210	Linux	10.20.2.250	0	0	0	0
211	Linux	10.20.7.42	0	0	0	1
212	Linux	10.20.7.43	0	0	0	1
213	Linux	10.20.7.45	0	0	0	2
214	aruba-master.bajajauto.co.in	10.20.7.46	0	0	0	2
215	Linux	10.20.7.47	0	0	0	2
216	hpn.bajajauto.co.in	10.20.2.211	0	0	0	4
217	cnsrv1.bajajauto.co.in	10.20.2.212	0	0	0	4
218	Windows	10.20.4.20	0	3	0	1
219	Windows	10.20.4.2	0	1	0	0
220	Windows	10.20.4.180	0	0	0	0
221	10.124.44.52	10.124.44.52	0	0	0	0
222	BALAKDLP03	10.20.2.198	0	0	0	1
223	BALAKSCCMAPP01	10.20.2.140	0	0	0	1
224	balwlsccmdp01.bajajauto.co.in	10.12.104.250	0	0	0	1
225	Linux	172.16.1.121	0	0	0	0
226	Linux	172.16.1.205	0	0	0	0
227	Linux	172.16.1.206	0	0	0	0
228	balwjbstdb02.bajajauto.co.in	10.12.104.251	0	0	0	2
229	10.13.14.1	10.13.14.1	0	0	0	1
230	10.13.14.35	10.13.14.35	0	0	0	0
231	10.20.10.168	10.20.10.168	0	0	0	0
232	10.20.10.169	10.20.10.169	0	0	0	0
233	10.20.10.170	10.20.10.170	0	0	0	0
234	10.20.10.171	10.20.10.171	0	0	0	0
235	10.20.10.172	10.20.10.172	0	0	0	0
236	10.20.10.173	10.20.10.173	0	0	0	0
237	10.20.10.174	10.20.10.174	0	0	0	0
238	10.20.10.175	10.20.10.175	0	0	0	0
239	10.20.10.176	10.20.10.176	0	0	0	0
240	10.20.10.177	10.20.10.177	0	0	0	0
241	10.20.10.178	10.20.10.178	0	0	0	0
242	vhbalboddb01.bajajauto.co.in	10.20.10.240	0	0	0	0
243	vhbalpoqjp01.dc.hec.bajajauto.co.in	10.20.10.132	0	0	0	0
244	172.16.1.207	172.16.1.207	0	0	0	1
245	172.16.1.208	172.16.1.208	0	0	0	0
246	10.20.2.1	10.20.2.1	0	0	0	0
247	10.20.2.2	10.20.2.2	0	0	0	0
248	10.20.2.3	10.20.2.3	0	0	0	0
249	BALREMEDYAPP	10.20.2.55	0	0	0	0

250	10.20.10.194	10.20.10.194	0	0	0	2
251	10.20.10.195	10.20.10.195	0	0	0	2
252	10.11.0.1	10.11.0.1	0	0	0	0
253	10.11.0.33	10.11.0.33	0	0	0	0
254	ak-pcs-3144.bajajauto.co.in	10.11.0.50	0	0	0	1
255	10.11.0.65	10.11.0.65	0	0	0	0
256	10.11.0.129	10.11.0.129	0	0	0	0
257	10.12.104.10	10.12.104.10	0	0	0	1
258	10.12.104.12	10.12.104.12	0	0	0	0
259	10.12.104.18	10.12.104.18	0	0	0	0
260	10.12.104.20	10.12.104.20	0	0	0	0
261	balwjeptw01.bajajauto.co.in	10.12.104.48	0	0	0	4
262	balwj4whpaint01.bajajauto.co.in	10.12.104.58	0	0	0	0
263	balckmesves01.bajajauto.co.in	10.13.14.73	0	0	0	0
264	balckmesves02.bajajauto.co.in	10.13.14.74	0	0	0	0
265	balckavl01.bajajauto.co.in	10.13.14.82	0	0	0	2
Total			**0**	**6**	**15**	**237**

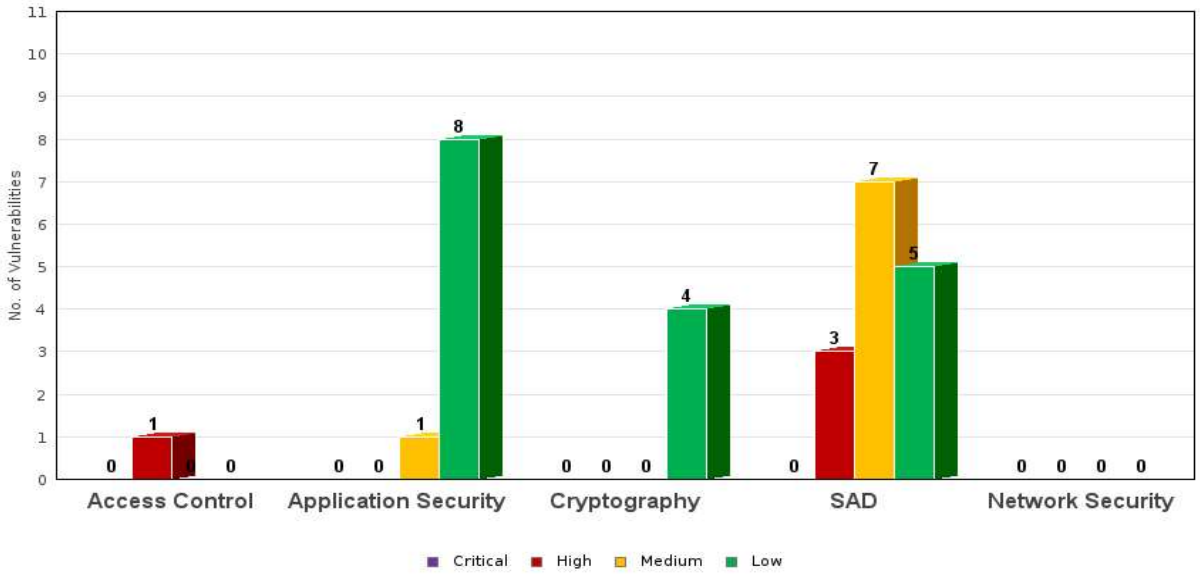
4. Executive Summary

During the assessment, Sumeru found **0 Critical**, **4 High**, **8 Medium** and **17 Low** unique vulnerabilities. Each identified vulnerability is present in one or more systems as shown in the graph below.

Vulnerable Systems in External & Internal Networks



The identified vulnerabilities are categorized under different security domains



*SAD: Secure Architecture Design

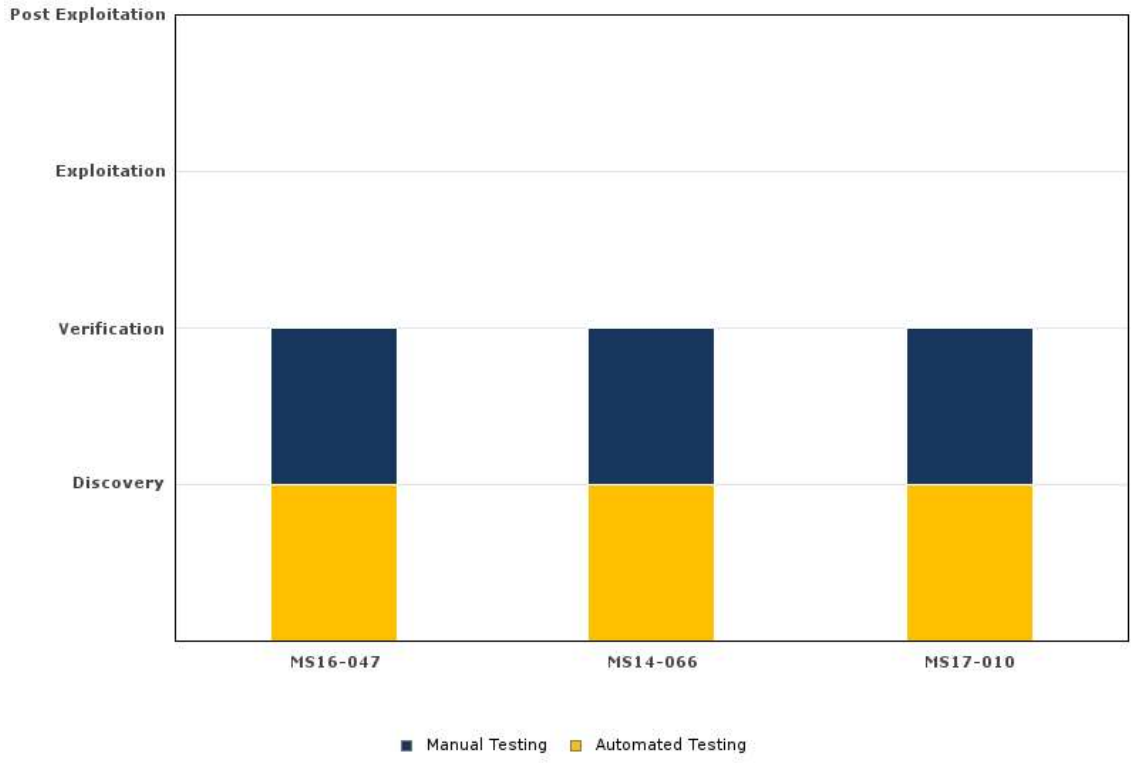
From the CVSS score across different domains, the cumulative average score and the grade is calculated and displayed below (The grading is derived from CVSS)

Grade	C+
Cumulative Average Score	17

Grading Scale	A+	A	A-	B+	B	B-	C+	C	C-	D+	D	D-
Score Scale	40 - 38	37 - 35	33 - 28.5	27 - 24	23.5 - 19	18.5 - 18	17.5 - 13	12.5 - 12	11.5 - 8	7 - 5	4.5 - -7	-7.5 - -25

Please Refer:
ANNEXURE – C (Sumeru's Grading Methodology) for grade calculation and domains description.
ANNEXURE – D (CVSS Score) for CVSS scoring methodology.

Manual Testing Vs Automated Testing



The graph above shows the vulnerabilities, and whether they were discovered, verified and exploited manually or with an automated tool.

5. Conclusion

Based on the findings and our experience working with Bajaj Auto, in order to ensure a comprehensive security we conclude the following:

Activities	Recommendation
Immediate	• Create a vulnerability remediation plan based on priority/criticality and fix the vulnerabilities within **4 weeks** after the report is received. • Informing Sumeru after fixing the vulnerabilities and plan for Post Remediation Assessment(PRA)
Ongoing	1. The **High** vulnerability found in **Access Control** can be addressed by ◦ Implementation of an effective access control policy. ◦ Access control can also be made effective by monitoring and logging. ◦ Applying authentication and disabling all the unauthenticated access to services. (e.g., default app creds) 2. The **Medium** vulnerability found in **Application Security** can be addressed by ◦ Periodic review of the effectiveness in the existing access control policy. ◦ Effective monitoring and logging of access controls. ◦ We recommend to disabling directory listing in the webserver. ◦ Following the guidelines given by OWASP (Open Web ApplicationSecurity Project) for securing the applications. 3. The **High and Medium** vulnerabilities are found in **Secure Architecture Design** can be addressed by ◦ Timely patching of the system by implementing effective patch management policy. ◦ Keeping an eye on the vendor advisories which are getting releases with time (e.g. Microsoft Patches, ssl patches). ◦ Implementation of vulnerability management plan to deal with upcoming vulnerabilities.

6. Vulnerability Summary for BA

Note: Only high risk vulnerabilities are mentioned here.

Issue	Description	Business Impact
MS16-047 Security Update for SAM and LSAD Remote Protocols	The vulnerability is caused by the way the SAM and LSAD remote protocols establish the Remote Procedure Call (RPC) channel. An attacker who successfully exploited this vulnerability could gain access to the SAM database.	A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.
MS14-066_Vulnerability in Schannel Could Allow Remote Code Execution	The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package.	This vulnerability can lead to loss of confidentiality, integrity and availability.
MS17-010 (ETERNALBLUE)	The remote code execution vulnerability exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server, where an attacker who successfully exploiting the vulnerability could gain the ability to execute code on the target server	An attacker can compromise the system by executing arbitrary code leading to system compromise.

7. Detailed Report

7.1 External Testing (0 Critical,0 High, 3 Medium, 6 Low)

MEDIUM	V1	PHP Multiple Vulnerabilities
CVSS Base	6.1	**Classification** CVE-2016-1283, CVE-2017-16642
Description	The remote web server uses a version of PHP that is affected by multiple vulnerabilities.	
Impact	An attacker can able to perform a denial of service, buffer overflow, arbitrary command injection, and remote code execution.	
Affected IPs		

IP Address	Port	Affected version
External		
104.211.99.99	80	7.1.8
104.211.98.34	80	7.1.8

Workaround/ Solution
We recommend upgrading the PHP to version 8.0.2 and recommend hiding version information also.
Proof Of Concept / Steps to Reproduce
N/A
Tools Used
Nessus

MEDIUM	V2	Apache Multiple Vulnerabilities	
CVSS Base	5.3	**Classification**	CVE-2018-17189, CVE-2018-17199, CVE-2019-0190
Description	The version of Apache running on the remote host is affected by the Apache Multiple vulnerabilities.		
Impact	An attacker can use the existing vulnerabilities to cause the denial of service this information to do further attacks against the system.		

Affected IPs

IP Address	Port	Affected version
External		
104.211.99.99	80	2.4.34
104.211.98.34	80	2.4.27

Workaround/ Solution

We recommend upgrading the Apache to version 2.4.46 and recommend hiding version information in the response header.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

MEDIUM	V3	PhpMyAdmin page Available Publicly	
CVSS Base	4.3	**Classification**	CVE-2019-6798
Description	PhpMyAdmin is publicly available on the target server and the version of it is affected by multiple vulnerabilities like SQL injection (SQLi), arbitrary file read using which an attacker can get the information about the application to perform further attacks.		
Impact	An attacker can run brute force attack against the PhpMyAdmin and find the password and can access, modify or delete all MySQL databases.		
Affected IPs	**IP Address**	**Port**	
	External		
	52.172.218.153	80	

Workaround/ Solution

We recommend restricting the access of sensitive URLs from the public user by forced browsing and also upgrade to the latest phpMyAdmin version.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

N/A

LOW	V4	HTTP Clear Text Credentials	
CVSS Base	3.8	**Classification**	CWE: 522
Description	The web application sends data in clear text which can be easily sniffed by an attacker.		
Impact	An attacker could sniff the sensitive information like usernames/passwords. This might lead to identity theft and potential compromise of the server.		

Affected IPs

IP Address	Port
External	
52.172.194.178	80
52.172.218.153	80
104.211.99.99	80
104.211.98.34	80

Workaround/ Solution

We recommend using HTTPS instead of HTTP.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

LOW	V5	Clickjacking Vulnerability	
CVSS Base	3.7	**Classification**	CWE: 693
Description	Clickjacking (User Interface redress attack) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on.		
Impact	Victim could potentially reveal confidential information while clicking on seemingly innocuous web pages.		
Affected IPs			

IP Address	Port
Extenal	
52.172.218.153	80
52.172.194.178	80

Workaround/ Solution

We recommend implementing header “X-FRAME-OPTIONS”

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

LOW	V6	SSL Weak Ciphers Supported	
CVSS Base	3.4	**Classification**	CVE-2016-2183
Description	The remote host supports the use of SSL ciphers that offer weak encryption.		
Impact	This is considerably easier to exploit if the attacker is on the same physical network.		
Affected IPs	**IP Address**	**port**	
	External		
	13.71.18.246	443	

Workaround/ Solution

We recommend disabling the supported Weak Ciphers and disable the protocol SSLv3, TLSv1.0 in the system.
Windows: Start Registry Editor (Regedt32.exe), and then locate the following registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers
Ref:
https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-ofcertaincryptographicalgorithms-and-protoc

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus, Nmap

LOW	V7	JQuery Outdated	
CVSS Base	3.4	**Classification**	CVE-2020-11022
Description	The installed version of the JQuery is no longer supported by the vendor.		
Impact	There will be no fixes released by the vendor for future security vulnerabilities.		
Affected IPs	**IP Address**	**Port**	**Affected version**
	External		
	104.211.99.99	80	3.2.1
Workaround/ Solution			
We recommend updating to the latest version 3.5.1 JQuery available with the vendor.			
Proof Of Concept / Steps to Reproduce			
N/A			
Tools Used			
Nessus			

LOW	V8	TRACE Method Enabled	
CVSS Base	2.3	**Classification**	CVE-2003-1567
Description	HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method.		
Impact	Successful exploits may allow an attacker to compromise user accounts by gaining access to sensitive header information. This issue may be combined with other attacks such as cross-site request forgery attacks		
Affected IPs	**IP Address**	**Port**	
	External		
	104.211.98.34	80	
	104.211.99.99	80	
Workaround/ Solution			
We recommend disabling the TRACE Method on the web server.			
Proof Of Concept / Steps to Reproduce			
N/A			
Tools Used			
Nessus			

LOW	V9	Directory Browsing Enabled	
CVSS Base	2.3	**Classification**	CWE-548
Description	Directory browsing is enabled on server which displays a web page that lists the contents of a directory which contains listing of internal directories having sensitive information files.		
Impact	An attacker could browse through the files and folder on remote host without any authentication. Sensitive files and directories may be disclosed to the attacker.		
Affected IPs			

IP Address	Port
External	
52.172.218.153	80
52.172.194.178	80
104.211.99.99	80

Workaround/ Solution

We recommend restricting directory browsing from the web server configuration.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

7.2 Internal Testing (0 Critical,4 High, 5 Medium, 11 Low)

HIGH	V10	MS16-047 Security Update for SAM and LSAD Remote Protocols	
CVSS Base	7.7	**Classification**	CVE-2016-0128
Description	The vulnerability is caused by the way the SAM and LSAD remote protocols establish the Remote Procedure Call (RPC) channel. An attacker who successfully exploited this vulnerability could gain access to the SAM database.		
Impact	A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.		
Affected IPs	**IP Address**	**Port**	
	Internal		
	10.20.4.2	49159	
	10.20.4.2	49155	
	10.20.4.20	49155	
	10.20.4.20	49158	
Workaround/ Solution			
Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.			
Proof Of Concept / Steps to Reproduce			
N/A			
Tools Used			
N/A			

HIGH	V11	MS14-066_Vulnerability in Schannel Could Allow Remote Code Execution	
CVSS Base	7.6	**Classification**	CVE-2014-6321
Description	The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package.		
Impact	An attacker who successfully exploited this vulnerability could execute arbitrary code in the context of the System account.		
Affected IPs	**IP Address**	**Port**	
	Internal		
	10.20.4.20	443	

Workaround/ Solution

Microsoft has released a set of patches for Windows in the given below URL:
https://technet.microsoft.com/en-us/library/security/MS14-066

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

HIGH	V12	MS17-010 (ETERNALBLUE)	
CVSS Base	7.6	**Classification**	CVE-2017-0148
Description	The remote code execution vulnerability exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server, where an attacker who successfully exploiting the vulnerability could gain the ability to execute code on the target server		
Impact	An attacker could execute arbitrary code with SYSTEM level previleges and compromise the system. Further attacker can gather sensitive information like password hashes to log on to the other systems in the network which are configured with the same password.		
Affected IPs	**IP Address**	**Port**	
	Internal		
	10.20.4.20	445	
Workaround/ Solution			
We recommend to apply the following missing patches https://technet.microsoft.com/library/security/MS17-010			
Proof Of Concept / Steps to Reproduce			
N/A			
Tools Used			
Nessus			

HIGH	V13	Anonymous FTP Login Enabled	
CVSS Base	7.6	**Classification**	CVE-1999-0497
Description	It is possible to login to the FTP server using anonymous login.		
Impact	An attacker could access the FTP server to upload malicious files and misusing the FTP server to launch further attacks.		
Affected IPs	**IP Address**	**Port**	
	Internal		
	10.20.2.152	21	
	10.20.2.161	21	
Workaround/ Solution			
We recommend disabling anonymous logins and implementing strong password policy.			
Proof Of Concept / Steps to Reproduce			
N/A			
Tools Used			
Nmap			

MEDIUM	V14	Microsoft SQL Server Unsupported Version Detection	
CVSS Base	6.8	**Classification**	CVE-2019-1068
Description	The installed version of Microsoft SQL Server is no longer supported by the vendor.		
Impact	Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.		

Affected IPs

IP Address	Port	Affected version
Internal		
10.12.104.33	1433	11.0.3000.0
10.12.104.33	49666	12.0.2000.0
10.12.104.51	63370	11.0.2100.0
10.20.2.202	1433	11.0.6020.0
10.20.2.229	60280	10.0.2531.0

Workaround/ Solution

We recommend upgrading to the latest version Microsoft SQL Server 2019

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

MEDIUM	V15	PHP Unsupported Version	
CVSS Base	6.6	**Classification**	CVE-2018-10545
Description	The PHP version installed in remote host is obsolete & no longer supported by its vendor.		
Impact	Use of unsupported version of PHP can result in security vulnerabilities due to the unavailability of patches.		

Affected IPs

IP Address	Port	Affected version
Internal		
172.16.1.140	80	5.6.36-1+ubuntu16.04.1+deb.sury.org+1
172.16.1.140	443	5.6.36-1+ubuntu16.04.1+deb.sury.org+1

Workaround/ Solution

We recommend upgrading to the latest version 8.0.2 and recommend hiding version information also

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

MEDIUM	V16	VMware vCenter Multiple Vulnerabilities	
CVSS Base	5.3	**Classification**	CVE-2019-5534, CVE-2019-5532, CVE-2019-5531
Description	VMware vCenter server is running on target system which allows for management of multiple ESX servers and virtual machines. vCenter server is affected by multiple vulnerabilities such as: • Arbitrary Code Execution • Denial of Service • An information disclosure vulnerability Vulnerabilities listed for the server allow a malicious user to run unwanted code on target and disrupt running services.		
Impact	Listed vulnerabilities allow a malicious user to perform execution of unauthorized commands or code and also allows to shutdown the services running on target system. Which results in unavailability of services or virtual machines and loss of sensitive information.		
Affected IPs	**IP Address**	**Port**	**Affected version**
	Internal		
	10.12.104.25	443	6.5.0 build-4602587
	10.12.104.26	443	6.5.0 build-4602587
	10.20.2.121	443	6.5 build 14020092

Workaround/ Solution

We recommend upgrading VMware vCenter Server to version 6.7.0.13000.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

MEDIUM	V17	Jenkins Multiple Vulnerabilities	
CVSS Base	4.3	**Classification**	CVE-2019-1003004
Description	The version of Jenkins running on the remote web server is affected by multiple vulnerabilities.		
Impact	An attacker could cause denial of service and other application attacks causing loss of availability and confidentiality.		
Affected IPs			

IP Address	Port	Affected version
Internal		
10.20.2.152	8080	2.138.1

Workaround/ Solution

We recommend upgrading Jenkins to version 2.263.4 and recommend hiding version information also.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

MEDIUM	V18	Apache Tomcat Multiple Vulnerabilities	
CVSS Base	4.3	**Classification**	CVE-2018-8034, CVE-2020-13935, CVE-2020-13934
Description	The version of Apache Tomcat running on the remote host is affected by Multiple vulnerabilities.		
Impact	An attacker can use the existing vulnerabilities to cause the denial of service and helps to do further attacks against the system.		

Affected IPs

IP Address	Port	Affected version
Internal		
10.20.2.122	8080	7.0.85
10.12.104.254	8080	8.5.35
10.20.2.156	9080	7.0.55
10.20.2.155	443	8.0.36
10.20.2.161	8080	8.0.0-RC5
10.20.2.155	8443	7.0.65

Workaround/ Solution

We recommend upgrading the Apache Tomcat to version 10.0.2 and recommend hiding version information also.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

LOW	V19	HTTP Clear Text Credentials	
CVSS Base	3.8	**Classification**	CWE:522
Description	The web application sends data in clear text which can be easily sniffed by an attacker.		
Impact	An attacker could sniff the sensitive information like usernames/passwords. This might lead to identity theft and potential compromise of the server.		

Affected IPs

IP Address	Port
Internal	
10.20.2.124	80
10.20.2.161	80
10.20.2.156	80
10.20.2.133	80
10.20.2.133	8080
10.20.2.108	80
10.20.2.113	3080
10.20.2.108	8000
10.20.2.122	8080
10.20.2.161	8080
10.20.2.108	8888
10.20.2.111	9090
10.12.104.254	8080
10.20.2.87	80
10.20.2.234	81
10.20.2.86	3081
10.20.2.83	4080
10.20.2.86	4080
10.20.2.86	3080
10.20.2.95	3080
10.20.2.228	3080
10.12.104.58	81,83
10.12.104.48	5202
10.20.2.152	8080
10.20.32.40	8080

Workaround/ Solution

We recommend using HTTPS instead of HTTP.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

LOW	V20	SSH Weak Algorithm Supported	
CVSS Base	3.7	**Classification**	CVE-2008-5161
Description	The SSH server is configured to allow weak encryption algorithms.		
Impact	This is considerably easier to exploit if the attacker is on the same physical network.		

Affected IPs

IP Address	Port
Internal	
10.20.2.105	22
10.20.2.161	22
10.20.2.169	22
10.20.7.45	22
10.20.7.46	22
10.20.7.47	22
10.20.2.211	22
10.20.2.212	22
10.20.10.33	22
10.20.10.51	22
10.20.2.87	22
10.20.2.5	22
10.12.104.35	22

Workaround/ Solution

We recommend disabling the weak supported algorithms and remove CBC mode ciphers [arcfour,arcfour128,arcfour256,3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast1 28-cbc,hmac-md5,hmac-md5-96,hmac-md5-96-etm@openssh.com,hmacmd5-etm@openssh.com,hmacsha1-96,hmac-sha1-96-etm@openssh.com,hmac-md5] and Remove the above mentioned ciphers and add CTR ciphers [aes128-ctr,aes192-ctr,aes256-ctr] in the config file.
Windows:Start Registry Editor (Regedt32.exe), and then locate the following registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\CipherSuites
Ref:
https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-ofcertaincryptographicalgorithms-and-protoc
Linux: /etc/ssh/sshd_config Remove the above mentioned ciphers and add CTR ciphers [aes128-ctr,aes192-ctr,aes256-ctr] in the config file.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus, Nmap

LOW	V21	Clickjacking Vulnerability	
CVSS Base	3.7	**Classification**	CWE: 693
Description	Clickjacking (User Interface redress attack) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on.		
Impact	Victim could potentially reveal confidential information while clicking on seemingly innocuous web pages.		

Affected IPs

IP Address	Port
Internal	
10.20.2.224	80
10.20.2.161	80
10.20.2.108	80
10.20.2.224	443
10.20.2.113	3080
10.20.2.122	8080
10.20.2.161	8080
10.20.2.111	9090
10.12.104.254	8080
10.20.32.40	8080
10.20.2.61	9050
10.20.2.234	82
10.20.2.86	3080
10.20.2.95	3080
10.20.2.228	3080
10.20.2.86	3081
10.20.2.86	4080
10.20.2.83	4080
10.20.2.23	8080

Workaround/ Solution

We recommend implementing header “X-FRAME-OPTIONS”

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

N/A

LOW	V22	SSL Weak Ciphers Supported	
CVSS Base	3.4	Classification	CVE-2016-2183
Description	The remote host supports the use of SSL ciphers that offer weak encryption.		
Impact	This is considerably easier to exploit if the attacker is on the same physical network.		

Affected IPs

IP Address	Port
Internal	
10.20.2.155	443
10.20.2.156	9443
10.20.2.105	443
10.20.2.156	443
10.20.2.216	2381
10.20.2.102	443
10.20.2.118	443
10.20.2.124	443
10.20.2.133	443
10.20.2.137	443
10.20.2.148	443
10.20.2.150	443
10.20.2.151	443
10.20.2.224	443
10.20.2.12	3389
10.20.2.19	3389
10.20.2.102	3389
10.20.2.108	3389
10.20.2.110	3389
10.20.2.111	3389
10.20.2.112	3389
10.20.2.113	3389
10.20.2.117	3389
10.20.2.118	3389
10.20.2.120	3389
10.20.2.122	3389
10.20.2.123	3389
10.20.2.124	3389
10.20.2.125	3389
10.20.2.126	3389
10.20.2.128	3389
10.20.2.133	3389
10.20.2.137	3389
10.20.2.148	3389
10.20.2.150	3389

10.20.2.151	3389
10.20.2.154	3389
10.20.2.155	3389
10.20.2.157	3389
10.20.2.158	3389
10.20.2.162	3389
10.20.2.164	3389
10.20.2.165	3389
10.20.2.168	3389
10.20.2.179	3389
10.20.2.180	3389
10.20.2.202	3389
10.20.2.203	3389
10.20.2.215	3389
10.20.2.216	3389
10.20.2.217	3389
10.20.2.224	3389
10.20.2.226	3389
10.20.2.164	636
10.20.2.164	3269
10.20.2.19	1433
10.20.2.123	1433
10.20.2.124	1433
10.20.2.133	1433
10.20.2.154	1433
10.20.2.162	1433
10.20.2.202	1433
10.20.2.155	9443
10.20.2.155	8443
10.20.2.24	1433
10.20.2.246	1433
10.20.2.50	50481
10.20.2.24	443
10.20.2.28	443
10.20.2.30	443
10.20.2.41	443
10.20.2.43	443
10.20.2.52	443
10.20.2.62	443
10.20.2.43	25
10.20.2.30	587
10.20.2.30	143
10.20.2.28	993
10.20.2.30	993

10.20.2.43	993
10.20.2.41	636
10.20.2.42	636
10.20.2.41	3269
10.20.2.42	3269
10.20.2.28	995
10.20.2.43	995
10.20.2.50	50518
10.20.2.24	3389
10.20.2.25	3389
10.20.2.26	3389
10.20.2.30	3389
10.20.2.37	3389
10.20.2.41	3389
10.20.2.42	3389
10.20.2.50	3389
10.20.2.52	3389
10.20.2.60	3389
10.20.2.61	3389
10.20.2.62	3389
10.20.2.72	3389
10.20.2.79	3389
10.20.2.81	3389
10.20.2.238	3389
10.20.2.246	3389
10.20.2.84	49737
10.20.2.229	60280
10.20.2.95	443
10.20.2.97	443
10.20.2.234	443
10.20.2.23	3389
10.20.2.82	3389
10.20.2.83	3389
10.20.2.84	3389
10.20.2.85	3389
10.20.2.86	3389
10.20.2.90	3389
10.20.2.91	3389
10.20.2.92	3389
10.20.2.95	3389
10.20.2.96	3389
10.20.2.97	3389
10.20.2.98	3389
10.20.2.228	3389

10.20.2.229	3389
10.20.2.233	3389
10.20.2.234	3389
10.20.2.235	3389
10.20.2.236	3389
10.20.2.23	1433
10.20.2.85	1433
10.20.2.96	1433
10.20.2.98	1433
10.20.2.23	8443
10.12.104.33	49666
10.12.104.51	63370
10.13.14.64	443
10.12.2.18	3389
10.12.2.28	3389
10.12.2.36	3389
10.12.2.249	3389
10.12.2.250	3389
10.12.104.25	3389
10.12.104.26	3389
10.12.104.33	3389
10.12.104.42	3389
10.12.104.46	3389
10.12.104.51	3389
10.12.104.55	3389
10.12.104.56	3389
10.12.104.57	3389
10.12.104.252	3389
10.12.104.253	3389
10.12.104.254	3389
10.13.14.33	3389
10.13.14.34	3389
10.13.14.36	3389
10.13.14.62	3389
10.13.14.63	3389
10.13.14.64	3389
10.12.104.33	1433
10.12.104.51	1433
10.12.104.252	1433
10.12.104.253	1433
10.12.104.254	1433
10.13.14.33	1433
10.13.14.62	1433
172.16.1.140	25

172.16.1.47	1433
10.22.1.6	1433
10.20.32.40	25
10.20.32.40	443
10.20.32.41	443
10.22.0.34	443
10.20.32.40	587
10.20.32.40	465
10.20.32.40	143
10.20.32.41	143
10.20.32.40	2525
10.20.32.40	993
10.20.32.41	993
172.16.1.45	636
10.20.32.36	636
10.20.32.40	110
10.20.32.41	110
172.16.1.45	3269
10.20.32.36	3269
10.20.32.40	995
10.20.32.41	995
172.16.1.34	3389
172.16.1.42	3389
172.16.1.45	3389
172.16.1.46	3389
172.16.1.47	3389
172.16.1.103	3389
10.20.32.34	3389
10.20.32.36	3389
10.20.32.40	3389
10.20.32.41	3389
10.22.0.32	3389
10.22.0.34	3389
10.22.0.119	3389
10.22.1.6	3389
10.22.1.29	3389
10.12.104.250	443
10.20.2.140	443
10.22.0.34	443
10.12.104.250	3389
10.20.2.140	3389
10.20.2.198	3389
10.22.0.34	3389
10.20.2.140	1433

10.20.2.211	443
10.20.2.212	443
10.20.4.20	443
10.12.104.35	443
10.11.0.22	443
10.12.104.35	443
10.12.104.35	5989
10.11.0.12	9043
10.12.104.48	50481
10.12.104.58	50481
10.12.104.251	50481
10.13.14.82	50481
172.16.1.207	443
10.20.2.24	443
10.20.2.54	443
10.20.10.194	443
10.20.10.195	443
10.20.10.194	636
10.20.10.195	636
10.20.10.194	389
10.20.10.195	389

Workaround/ Solution

We recommend disabling the supported Weak Ciphers and disable the protocol SSLv3, TLSv1.0 in the system.
Windows: Start Registry Editor (Regedt32.exe), and then locate the following registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers
Ref:
https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-ofcertaincryptographicalgorithms-and-protoc

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus, Nmap

LOW	V23	JQuery Outdated	
CVSS Base	3.4	**Classification**	CVE-2020-11022
Description	The installed version of the JQuery is no longer supported by the vendor.		
Impact	There will be no fixes released by the vendor for future security vulnerabilities.		

Affected IPs

IP Address	Port	Affected version
Internal		
10.20.2.133	80	1.10.2
10.20.2.133	443	1.10.2
10.20.2.113	3080	1.4.2
10.20.2.133	8080	1.10.2
10.20.2.108	8888	2.2.3
172.16.1.140	443	2.1.3
10.20.2.86	3080	1.8.3
10.20.2.228	3080	1.4.2
10.20.2.95	3080	1.4.2
10.20.2.86	3081	1.8.3
10.20.2.86	4080	1.4.2
10.20.2.83	4080	1.4.2

Workaround/ Solution

We recommend updating to the latest supported version 3.5.1

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

LOW	V24	SMB Signing Disabled	
CVSS Base	3.1	**Classification**	CVE-2016-2115
Description	The signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.		
Impact	Successful exploitation could allow remote attackers to gain sensitive information.		
Affected IPs			

IP Address	Port
Internal	
10.20.2.162	445
10.11.0.22	445
10.11.0.12	445
10.11.0.50	445
10.12.2.36	445
10.20.2.37	445

Workaround/ Solution

Enforce message signing in the host's configuration.
On Windows Servers:
* HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

LOW	V25	Apache Tomcat Default Files	
CVSS Base	3.0	**Classification**	CVE-2018-8014
Description	The Apache Tomcat servlet/JSP container has default files such as documentation, default Servlets and JSPs.		
Impact	An attacker can use files to guess the exact version of the Apache Tomcat which is running on this host and other useful information.		

Affected IPs

IP Address	Port
Internal	
10.20.2.161	8080
10.20.2.122	8080
10.12.104.254	8080
172.16.1.34	8080
10.20.2.156	9080

Workaround/ Solution

We recommend to remove default files, example JSPs and Servlets from the Tomcat Servlet/JSP container.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

LOW	V26	CBC Mode Ciphers Enabled	
CVSS Base	3.0	**Classification**	CWE-200
Description	The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.		
Impact	This may allow an attacker to recover the plaintext message from the ciphertext.		

Affected IPs

IP Address	Port
Internal	
10.20.2.152	22
10.20.7.42	22
10.20.7.43	22
10.20.7.45	22
10.20.7.46	22
10.20.7.47	22
10.20.2.211	22
10.20.2.212	22
10.20.10.33	22
10.20.10.51	22
10.20.7.44	22
10.20.7.50	22
172.16.1.140	22
172.16.1.141	22
10.20.2.87	22
10.12.104.10	22
10.13.14.1	22
10.20.2.5	22
10.12.104.10	22
10.12.104.35	22

Workaround/ Solution

We recommend to disable the CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus, Nmap

LOW	V27	POODLE Attack	
CVSS Base	2.3	**Classification**	CVE-2014-3566
Description	The POODLE attack takes advantage of the protocol version negotiation feature built into SSL/TLS to force the use of SSL 3.0 and then leverages this new vulnerability to decrypt select content within the SSL session. The decryption is done byte by byte and will generate a large number of connections between the client and server.		
Impact	This vulnerability allows an attacker to gain access to sensitive data passed within the encrypted web session, such as passwords, cookies and other authentication tokens that can then be used to gain more complete access to a website. Which leads to loss of sensitive information, loss of integrity and loss of user confidence.		

Affected IPs

IP Address	Port
Internal	
10.20.2.102	443
10.20.2.155	9443
10.20.2.156	9443
10.20.2.211	443
10.20.2.212	443
10.11.0.12	9043
10.12.104.48	1433
10.12.104.58	1433
10.12.104.251	1433
10.13.14.82	1433

Workaround/ Solution

It is recommended to use TLSv1.2 or above.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus, Nmap

LOW	V28	TRACE Method Enabled	
CVSS Base	2.3	**Classification**	CVE-2003-1567
Description	HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method.		
Impact	Successful exploits may allow an attacker to compromise user accounts by gaining access to sensitive header information. This issue may be combined with other attacks such as cross-site request forgery attacks		

Affected IPs

IP Address	Port
Internal	
10.20.2.87	80
10.20.2.87	8443
10.20.2.161	80
10.20.10.194	80
10.20.10.195	80
10.20.10.194	443
10.20.10.195	443

Workaround/ Solution

We recommend disabling the TRACE Method on the web server.

Proof Of Concept / Steps to Reproduce

N/A

Tools Used

Nessus

LOW	V29	FTP Clear Text Credentials	
CVSS Base	2.3	**Classification**	CWE-319
Description	It is found as the FTP service is being used in network which exchanges information in clear text which can be sniffed by the attacker.		
Impact	An attacker could gain FTP credentials and could gain the sensitive information from the FTP server.		
Affected IPs	**IP Address**	**Port**	
	Internal		
	10.20.2.128	21	
	10.20.2.238	21	
Workaround/ Solution			
We recommend disabling ftp and implementing SFTP or FTPS services.			
Proof Of Concept / Steps to Reproduce			
N/A			
Tools Used			
Nmap			

8. ANNEXURE – A (Tests Performed)

Test(s) performed and results obtained:

S/N	Test(s) Performed	Test Result	S/N	Test(s) Performed	Test Result
1	Configuration and Deploy Management Testing	Unsafe	2	Identity Management Testing	Safe
3	Authorization Testing	Safe	4	Data Validation Testing	Safe
5	Error Handling	Safe	6	Cryptography	Safe
7	Business Logic Testing	Safe	8	Client Side Testing	Unsafe
9	Test for Cleartext Credentials	Unsafe	10	Test for Patch Related Issues / Old Versions Usage	Unsafe
11	Test for SNMP service issues	Safe	12	Test For Password Files Public Availability	Safe
13	Test For Group Policy Preferences	Safe	14	Test for Unsupported Versions	Unsafe
15	Testing for Sensitive Data Exposure	Safe	16	Test for Authentication Bypass	Safe
17	Testing for Weak Password	Safe	18	Lack of Access Control	Safe
19	Test For Information Leakage	Safe	20	Network Time Protocol (NTP) vulnerability	Safe
21	SSH Weak Ciphers Enabled	Unsafe	22	Oracle Weblogic Multiple Vulnerabilities	Safe

9. ANNEXURE – B (Risk Classification)

Sumeru has classified the risk factors into four categories

CRITICAL CVSS (10 - 9)	A vulnerability causes loss of CIA [confidentiality | integrity | availability] is likely to have a catastrophic adverse effect on the organization business or individuals associated with the organization (e.g., employees, customers).
HIGH CVSS (8.9 - 7)	A vulnerability causes loss of CIA [confidentiality | integrity | availability] is likely to have a serious adverse effect on the organization business or individuals associated with the organization (e.g., employees, customers).
MEDIUM CVSS (6.9 - 4)	A vulnerability causes loss of CIA [confidentiality | integrity | availability] is likely to have only a limited adverse effect on the organization business or individuals associated with the organization (e.g., employees, customers).
LOW CVSS (3.9 - 0.1)	A vulnerability causes loss of CIA [confidentiality | integrity | availability] is likely to have only a limited effect on the organization business or individuals associated with the organization (e.g., employees, customers).

10. ANNEXURE – C (Sumeru's Grading Methodology)

1. During the Penetration Test Sumeru identifies vulnerabilities those are indexed above in the detailed report with **V1,V2,V3 … Vn.V1,V2,V3 … Vn** are the vulnerabilities discovered during the test affecting different system(s)/IP(s).
2. Then each discovered vulnerability is categorized in one of the five different security domains listed below based on the nature of the vulnerability:
    - **Access control:** Access control is the ability to permit or deny the use of a particular resource by a particular entity. (E.g.:- Access Control Lists in Operating systems, Routers, etc. In a Windows Server administrator have full access, normal user have restricted access)
    - **Application security:** Application security encompasses measures taken throughout the application's life-cycle to prevent exceptions in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgradation, or maintenance of the application.
    - **Cryptography:** Cryptography is used for encrypting sensitive information (passwords, Credit Card numbers, etc.). Within the context of any application-to-application communication, there are some specific security requirements, including:
        - Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
        - Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
        - Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
        - Non-repudiation: A mechanism to prove that the sender really sent this message.
    - **Secure Architecture Design:** Secure Architecture Design test consists of vulnerability assessment at implementation level of applications which in turn analyzes lapses in user access control, privilege escalations and lack of methodical defense/security approach across all levels (Physical, Network, application, etc.). It also analyzes the defense mechanism employed by firewall, antivirus, content management systems, etc.
    - **Network security:** Network security consists of the vulnerability assessment at network layer. There are two classes of vulnerability - mis-configuration, and firmware bugs - that can allow entry to non-authorized users. Mis-configuration can allow access to systems not authorized to be accessed: TCP port pings using port 80 are an example of this. Firmware are designed at embedded systems level and there is good deal of possibility of them containing the vulnerability at their application level. They can also contain vulnerabilities at the implementation level.

3. For each classified vulnerability, the CVSS (Common Vulnerability Scoring System) base score is calculated using CVSS Base score calculator. The screenshot below shows the CVSS base score

The CVSS base score for all the identified vulnerabilities in each the domains are calculated based on the above mentioned step.

1) Max CVSS score for each domain calculated as shown in the table below. The Max CVSS Score of SAD (Secure Architecture Design) is 8.80 calculated as MAX(3.1,4.7,8.8,4.3) = 8.8

S.NO	Access Control		Application Security		Cryptography		SAD		Network Security	
	Vuln.	CVSS Base Score	Vuln.	CVSS Base Score	Vuln.	CVSS Base Score	Vuln.	CVSS Base Score	Vuln.	CVSS Base Score
1	V5	7.1	V6	2.6	V3	6.3	V1	3.1	V2	5.3
2			V7	5	V4	3.1	V8	4.7		
3							V9	8.8		
4							V10	4.3		
5										
	MAX Score	7.10	MAX Score	5.00	MAX Score	6.30	MAX Score	8.80	MAX Score	5.30

2) Score is given to the each domain based on the below table.

Security	Strong	Adequate	Weak	Very Weak	None
CVSS	0	0.1 - 3.9	4.0 - 6.9	7.0 - 8.9	9.0 - 10.0
Risk	No Risk	Low	Medium	High	Critical

3) Finally Cumulative CVSS score is calculated by adding all the individual scores of each domain.

Classification Matrix						
Security Domains	Strong	Adequate	Weak	Very Weak	None	Score
Access Control	8	7	1	0.5	-5	0.5
Application Security	8	7	1	0.5	-5	1
Cryptography	8	7	1	0.5	-5	1
Secure Architecture Design	8	7	1	0.5	-5	0.5
Network Security	8	7	1	0.5	-5	1
Total Score						4

Based on the below table the final grade is assigned.

E.g. For the calculated Cumulative score of 4 the grade assigned would be D.

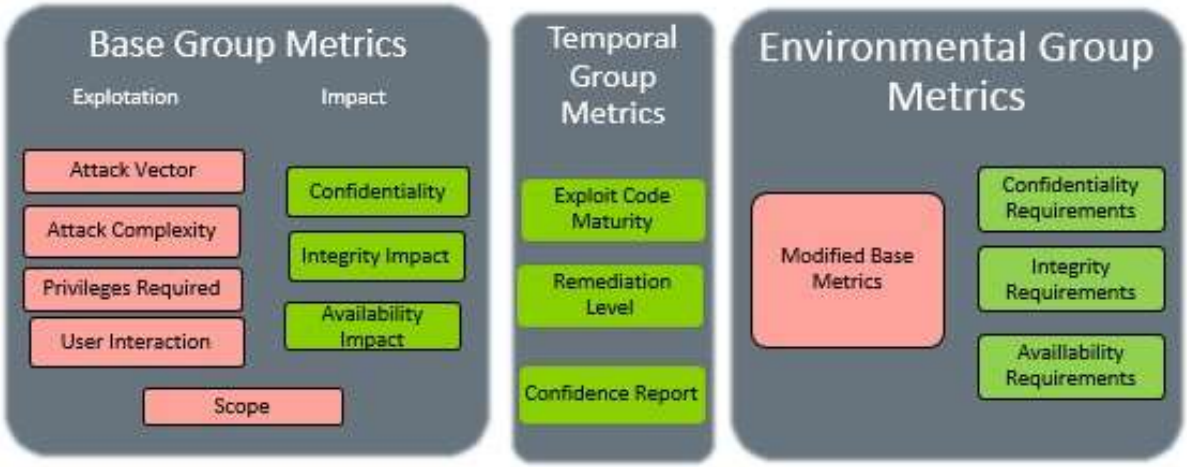
Grading Scale	A+	A	A-	B+	B	B-	C+	C	C-	D+	D	D-
Score Scale	40 - 38	37 - 35	33 - 28.5	27 - 24	23.5 - 19	18.5 - 18	17.5 - 13	12.5 - 12	11.5 - 8	7 - 5	4.5 - -7	-7.5 - -25

11. ANNEXURE – D (CVSS Score)

Sumeru uses CVSS risk classification metrics to identify and define risk factor for identified vulnerabilities in this report. The risk factor can be used to prioritize remediation activities for the identified vulnerabilities. For more details refer to http://www.first.org/cvss

What is CVSS?

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of 3 groups: Base, Temporal and Environmental. Each group produces a numeric score ranging from 0 to 10.



CVSS Metric Groups

These metric groups are described as follows:

Base: represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.

Temporal: represents the characteristics of a vulnerability that change over time but not among user environments.

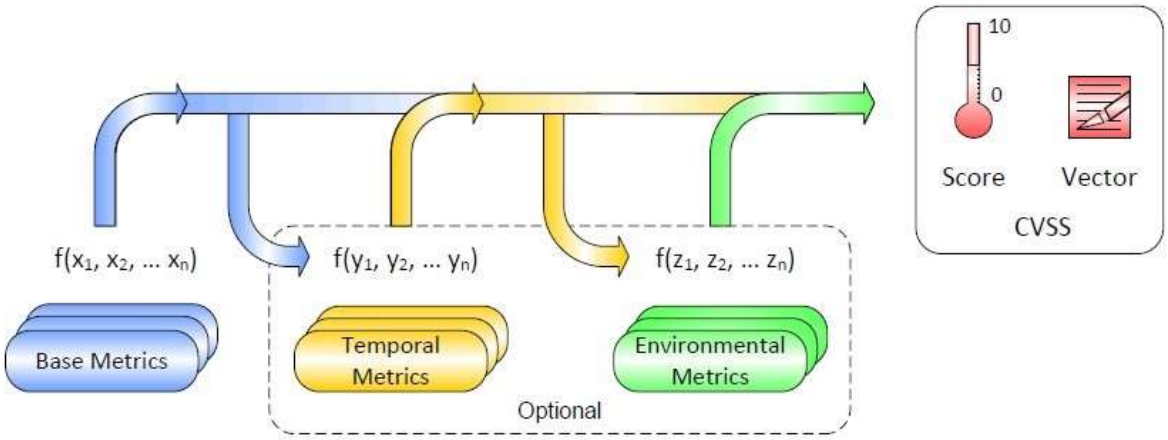
Environmental: represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities. The purpose of the CVSS base group is to define and communicate the fundamental characteristics of a vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability. **For this report we are only using the base grouping.** Optional later users can then invoke

the temporal and environmental groups to provide contextual information that more accurately reflects the risk to their unique environment. This allows them to make more informed decisions when trying to mitigate risks posed by the vulnerabilities.

How does CVSS work?

When the base metrics are assigned values, the base equation calculates a score ranging from 0 to 10, and a vector is created, as illustrated in below figure. The vector facilitates the "open" nature of the framework. It is a text string that contains the values assigned to each metric, and it is used to communicate exactly how the score for each vulnerability is derived.



CVSS Metrics and Equations

12. ANNEXURE – E (Glossary)

Vulnerability:

A bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability.

Hacker:

A word given by media to define what we will more accurately call attacker or intruder or cracker.

Threat:

The likelihood or frequency of a harmful event occurring.

Exploit:

A computer program or strategy to exploit a vulnerability.

Risk:

The relative impact that an exploited vulnerability would have to a user's environment.

FTP:

File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host or to another host over a TCP-based network.

SQL Injection:

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.

SMTP:

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks

Test Types

White-Box Testing

The penetration test team has complete carte blanche access to the target and has been supplied with network diagrams, hardware, operating system and application details etc., and prior to a test being carried out. This does not equate to a truly blind test but can speed up the process a great deal and leads to a more accurate results being obtained. The amount of prior knowledge leads to a test targeting specific operating systems, applications and network devices that reside on the network rather than spending time enumerating what could possibly be on the network. This type of test equates to a situation whereby an attacker may have complete knowledge of the internal network.

Black-Box Testing

No prior knowledge of a company network is known. In essence an example of this is when an external web based test is to be carried out and only the details of a website URL or IP address is supplied to the testing team. It would be their role to attempt to break into the company website/ network. This would equate to an external attack carried out by a malicious hacker.

Grey-Box Testing

The testing team would simulate an attack that could be carried out by a disgruntled, disaffected staff member. The testing team would be supplied with appropriate user level privileges and a user account and access permitted to the internal network by relaxation of specific security policies present on the network i.e. port level security.

13. References

1. CVSS Reference Guide https://www.first.org/cvss/user-guide
2. CVSS Calculator for calculating CVSS score https://www.first.org/cvss/calculator/3.0