Project Vulnerabilities Report

Project:	Administrative Machines
Submit by:	admin
Generated Time:	Oct. 2, 2018, 3:27 p.m.

Table Of Contents

Project Detailed Information

Information

Project:	Administrative Machines
Create by:	admin
Created Date:	Sept. 10, 2018, 3:29 a.m.
Updated Date:	Sept. 10, 2018, 3:29 a.m.

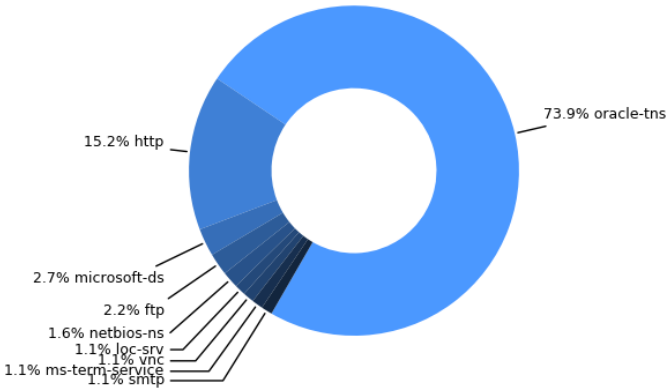
Description:
Scan administrative machines of TT1, ITKV

Vulnerabilities

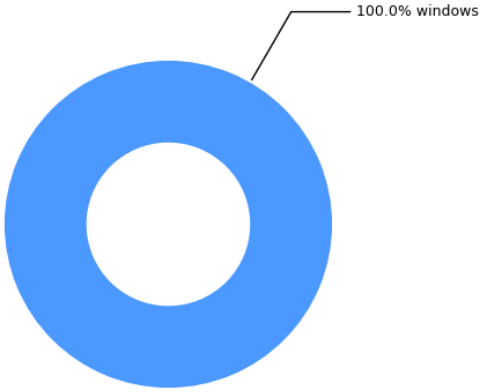
Overview

In this section, this report contains overview information that includes statistics by services (in graph-1), OS (in graph-2) and current categorized vulnerabilities (in graph-3) into groups:

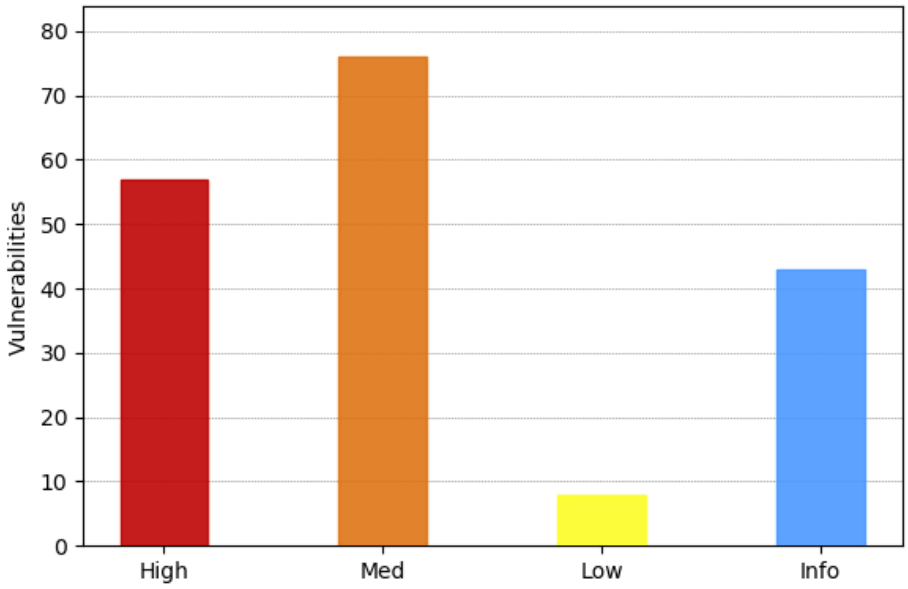
- **High Risk** - Exploitation of the vulnerability discovered on the system can directly lead to an attacker gaining privileged access (e.g. administrator, root) to the machine over a remote connection.
- **Medium Risk** - The vulnerability discovered on the system can directly lead to an attacker gaining non-privileged access (e.g. standard user) to the machine over a remote connection.
- **Low Risk** - The vulnerability discovered on the system provides enticement data to the attacker that may be used to launch a more informed attack against the target environment. In addition, the vulnerability may indirectly lead to an attacker gaining some form of access to the machine over a remote connection.
- **Informational Risk** - A finding on the system that provides data to an attacker that is of lesser value to an attacker than the enticement data provided by a low risk vulnerability.



Graph 1: Vulnerabilities statistic by services



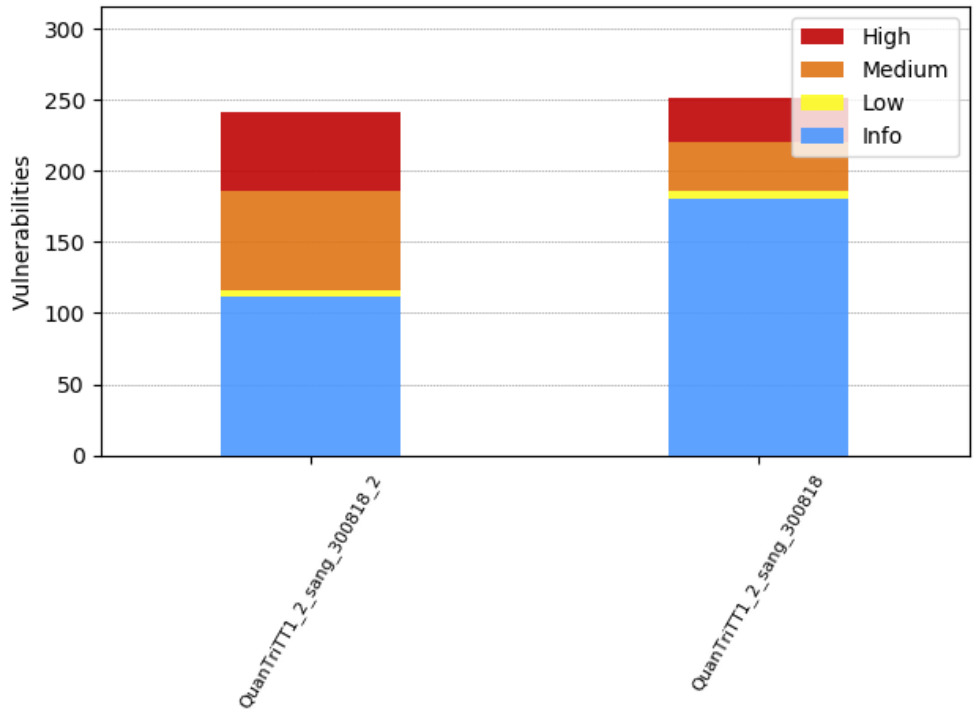
Graph 2: Vulnerabilities statistic by OS



Graph 3: Vulnerabilities statistic

Vulnerabilities by Scan Task

In this section, the report contains scan brief information of vulnerabilities that were discovered by this scan task.



Graph 4: Vulnerabilities of scanned hosts

Scan Result:

Scan Task	Start Time	Finished Time	Vulnerabilities			
			High	Med	Low	Info
QuanTriTT1_2_sang_300818_2	Aug. 30, 2018, 4:30 a.m.	Aug. 30, 2018, 4:56 a.m.	55	70	4	112
QuanTriTT1_2_sang_300818	Aug. 30, 2018, 4:30 a.m.	Aug. 30, 2018, 4:57 a.m.	31	34	6	180

Table 1: Vulnerabilities by Scan Task

Vulnerabilities by Host

In this section, the vulnerabilities is listed by host.

Scan Result:

Hostname	Ip Address	Vulnerabilities			
		High	Med	Low	Info
HO-CNTT-TT2-049	10.1.171.209	52	70	4	14
HO-CNTT-TT2-056	10.1.171.166	24	33	2	14
HO-CNTT-TT2-029	10.1.171.148	1	1	4	31
HO-CNTT-TT2-035	10.1.171.155	1	0	0	18
HO-CNTT-TT2-037	10.1.171.157	1	0	0	15
HO-CNTT-TT2-014	10.1.171.158	1	0	0	15
HO-CNTT-TT2-041	10.1.171.195	1	0	0	12
HO-CNTT-TT2-067	10.1.171.170	1	0	0	12
HO-CNTT-TT2-019	10.1.171.168	1	0	0	12
HO-CNTT-TT2-060	10.1.171.210	1	0	0	10
HO-CNTT-TT2-025	10.1.171.174	1	0	0	9
HO-CNTT-TT2-038	10.1.171.198	1	0	0	3
HO-CNTT-TT2-063	10.1.171.190	0	0	0	12
HO-CNTT-TT2-026	10.1.171.188	0	0	0	12
HO-CNTT-TT2-64	10.1.171.181	0	0	0	12
HO-CNTT-TT2-131	10.1.171.140	0	0	0	12
HO-CNTT-TT2-030	10.1.171.211	0	0	0	12
HO-CNTT-TT2-044	10.1.171.194	0	0	0	12
CNTT-TT2-EOD01	10.1.171.214	0	0	0	9
HO-CNTT-TT2-009	10.1.171.149	0	0	0	7
HO-CNTT-TT2-052	10.1.171.203	0	0	0	7
HO-CNTT-TT2-053	10.1.171.204	0	0	0	7
CNTT-TT2-EOD02	10.1.171.165	0	0	0	7

Hostname	Ip Address	Vulnerabilities			
		High	Med	Low	Info
HO-CNTT-TT2-005	10.1.171.141	0	0	0	7
HO-CNTT-TT2-054	10.1.171.176	0	0	0	6
HO-CNTT-TT2-016	10.1.171.147	0	0	0	5

Table 1: Vulnerabilities by Host