Your Company Name
Scan Results Trending Report
2.5.2017 - 2.8.2017

Introduction

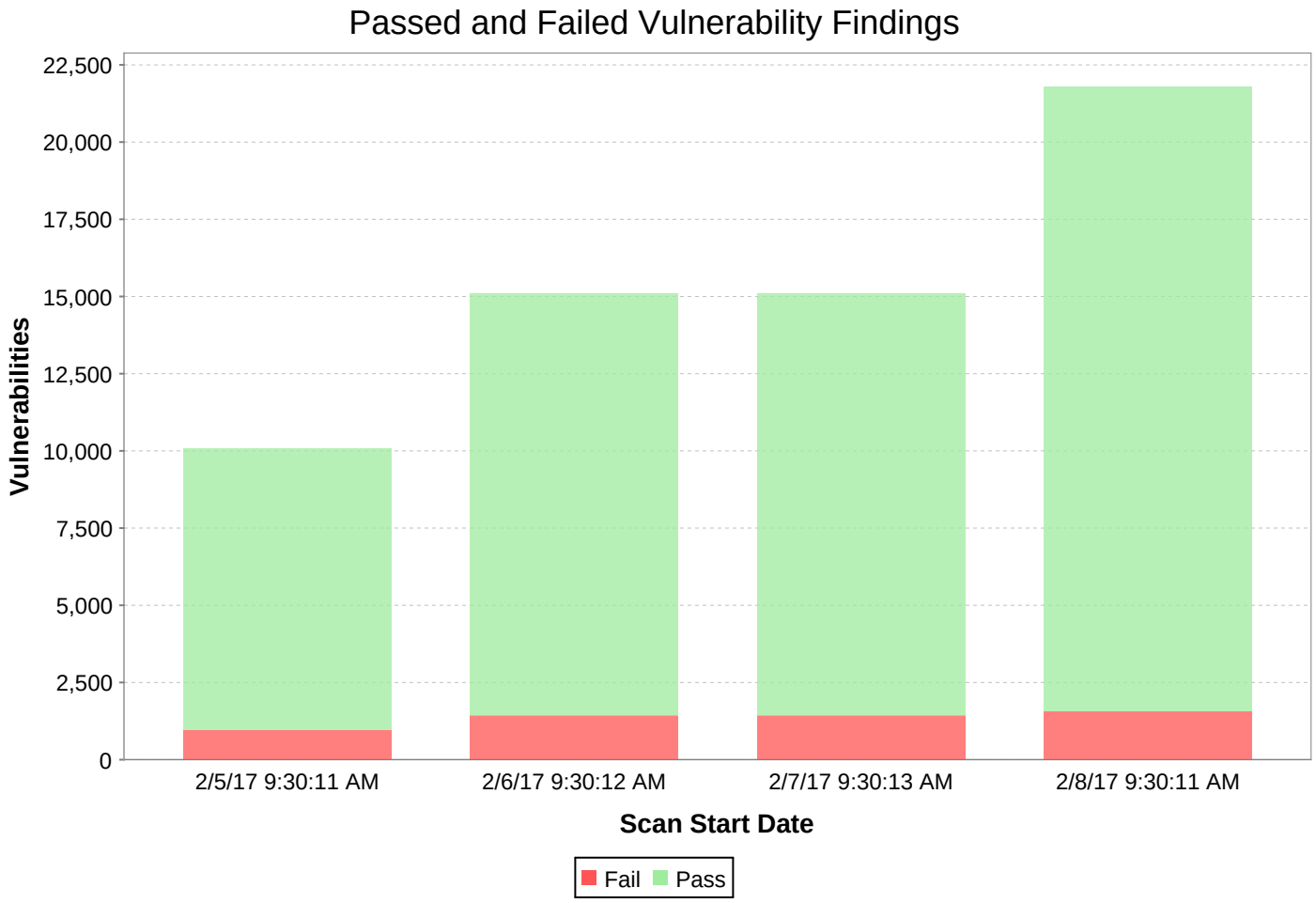
The results of each scan included in this report are presented in four different ways.

The **Passed and Failed Vulnerability Findings** chart includes all signatures that ran during the scan and indicates whether the host is vulnerable (represented as a fail) or is not vulnerable (represented as a pass) to each signature. As vulnerabilities are added to the scanner over time, the number of vulnerability findings will increase.

Each vulnerability included in the scan is given a high, medium, low, or no (none) severity based on how much damage the vulnerability could cause to a network if exploited. The **Failed and Error Vulnerabilities by Severity** chart includes only failed and error signatures found during the scan and indicates the severity levels of the vulnerabilities that failed during the scans.

As failed vulnerabilities are found during scans or as vulnerabilities result in errors, users can organize the work done to address the vulnerabilities by setting the results to different remediation statuses. Like the Failed and Error Vulnerabilities by Severity chart, the **Failed and Error Vulnerabilities by Remediation Status** chart shows only the failed and error signatures of the scan but indicates the work being done on the vulnerabilities by displaying the amount of vulnerabilities in each remediation status for the scan.

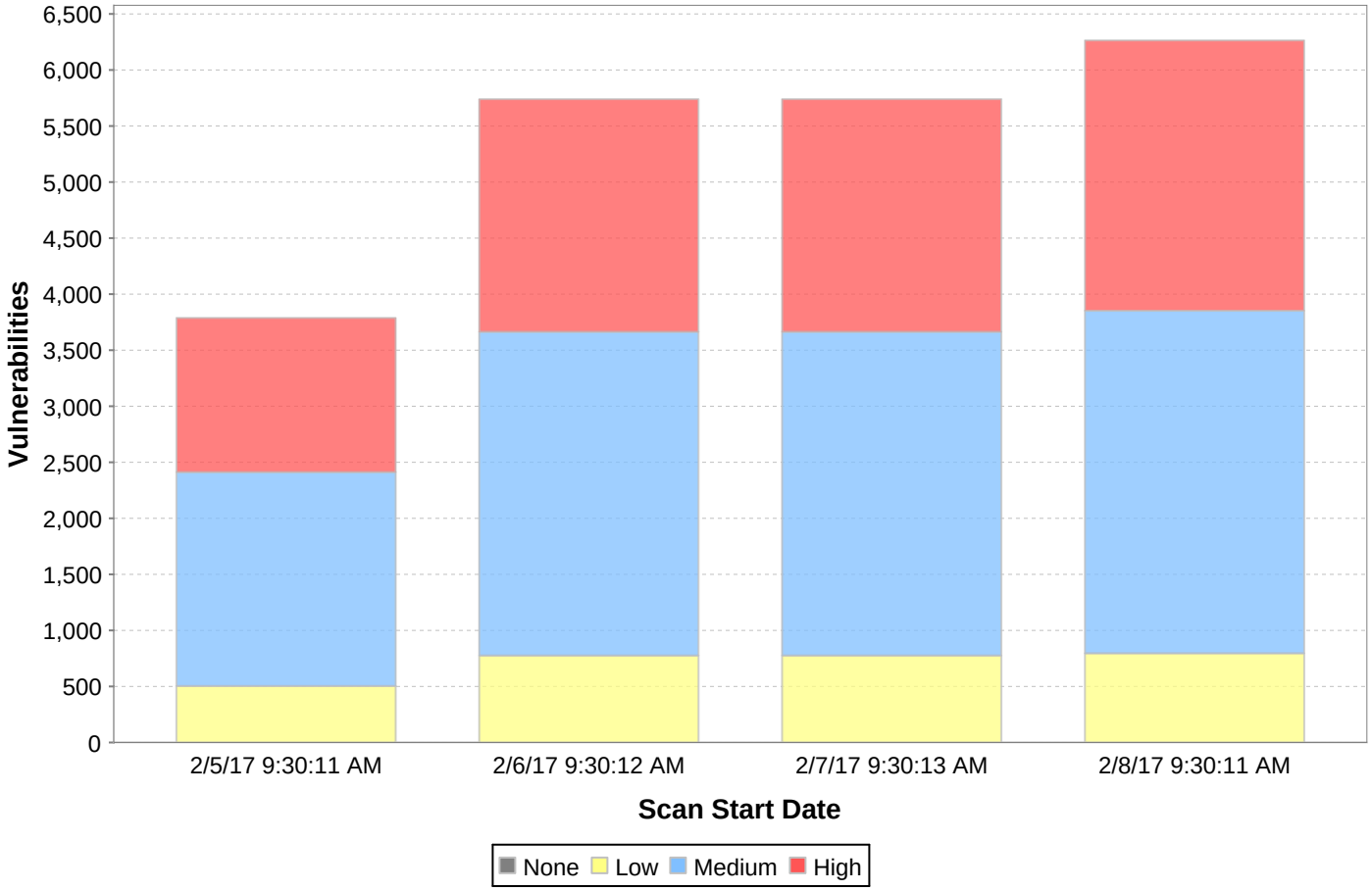
The **Number of Hosts Scanned** graph is a representation of the number of hosts included in the scan over time and provides context for the trends seen in the other three charts for the scan. If more hosts are made available to be scanned, the number of vulnerabilities will most likely increase. As hosts are removed from the network, the amount of vulnerability findings will most likely decrease.



The chart above shows the finding statuses of all vulnerabilities found during each scan event of the scan name "**feb 2017 daily scan**" . The finding statuses can be Pass, Fail, Error, or Unknown and Error/Unknown statuses are counted as failures. Only failed vulnerabilities require remediation. As new vulnerability definitions are added to the scanner, the amount of vulnerabilities represented in this graph will increase. Additionally, as hosts are added to and removed from the network being scanned, the amount of vulnerabilities shown may fluctuate. Counts are displayed in the table below.

	Error	Fail	Pass	Unknown	Total
2/5/17 9:30:11 AM	**0**	**5**	**9,125**	**942**	**10,072**
2/6/17 9:30:12 AM	**0**	**22**	**13,673**	**1,413**	**15,108**
2/7/17 9:30:13 AM	**0**	**22**	**13,673**	**1,413**	**15,108**
2/8/17 9:30:11 AM	**9**	**144**	**20,229**	**1,413**	**21,795**

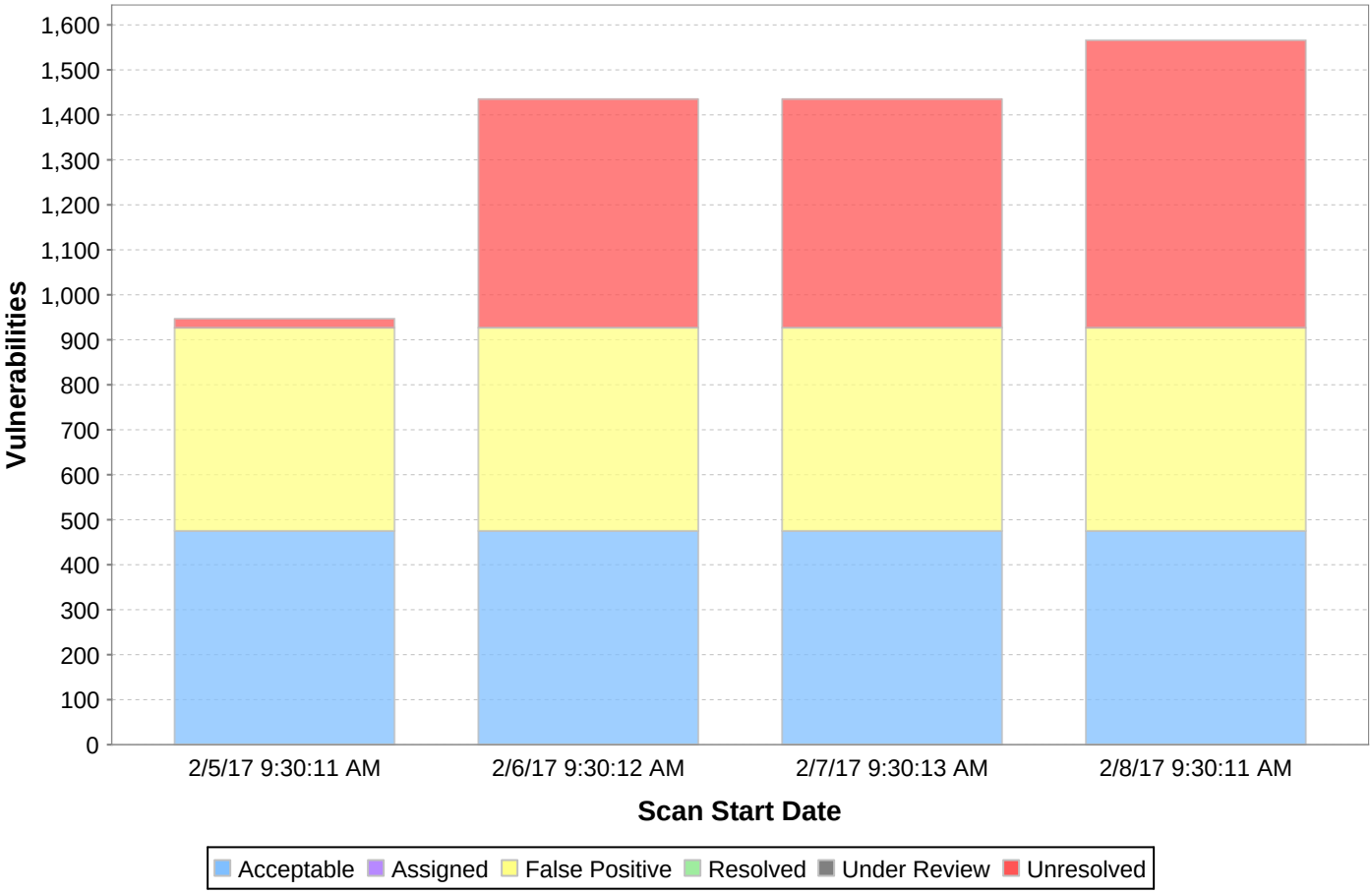
Failed and Error Vulnerabilities by Severity



The chart above shows the number of failed vulnerabilities found for each scan event of the scan named "**feb 2017 daily scan**" broken down by severity level. A vulnerability's severity level is considered high if it has a CVSS score greater than or equal to (>=) 7.0. Medium severity results include vulnerabilities with a CVSS score greater than or equal to (>=) 4.0 and less than (<) 7.0. Vulnerabilities with a low severity level have a CVSS score that is less than (<) 4.0. Vulnerabilities with no severity do not have a CVSS Score. As new vulnerability definitions are added to the scanner, the amount of vulnerabilities represented in this graph will increase. Additionally, as hosts are added to and removed from the network being scanned, the amount of vulnerabilities shown will fluctuate. Counts are displayed in the table below.

	None	Low	Medium	High
2/5/17 9:30:11 AM	**0**	**504**	**1,908**	**1,376**
2/6/17 9:30:12 AM	**0**	**776**	**2,888**	**2,076**
2/7/17 9:30:13 AM	**0**	**776**	**2,888**	**2,076**
2/8/17 9:30:11 AM	**0**	**796**	**3,056**	**2,412**

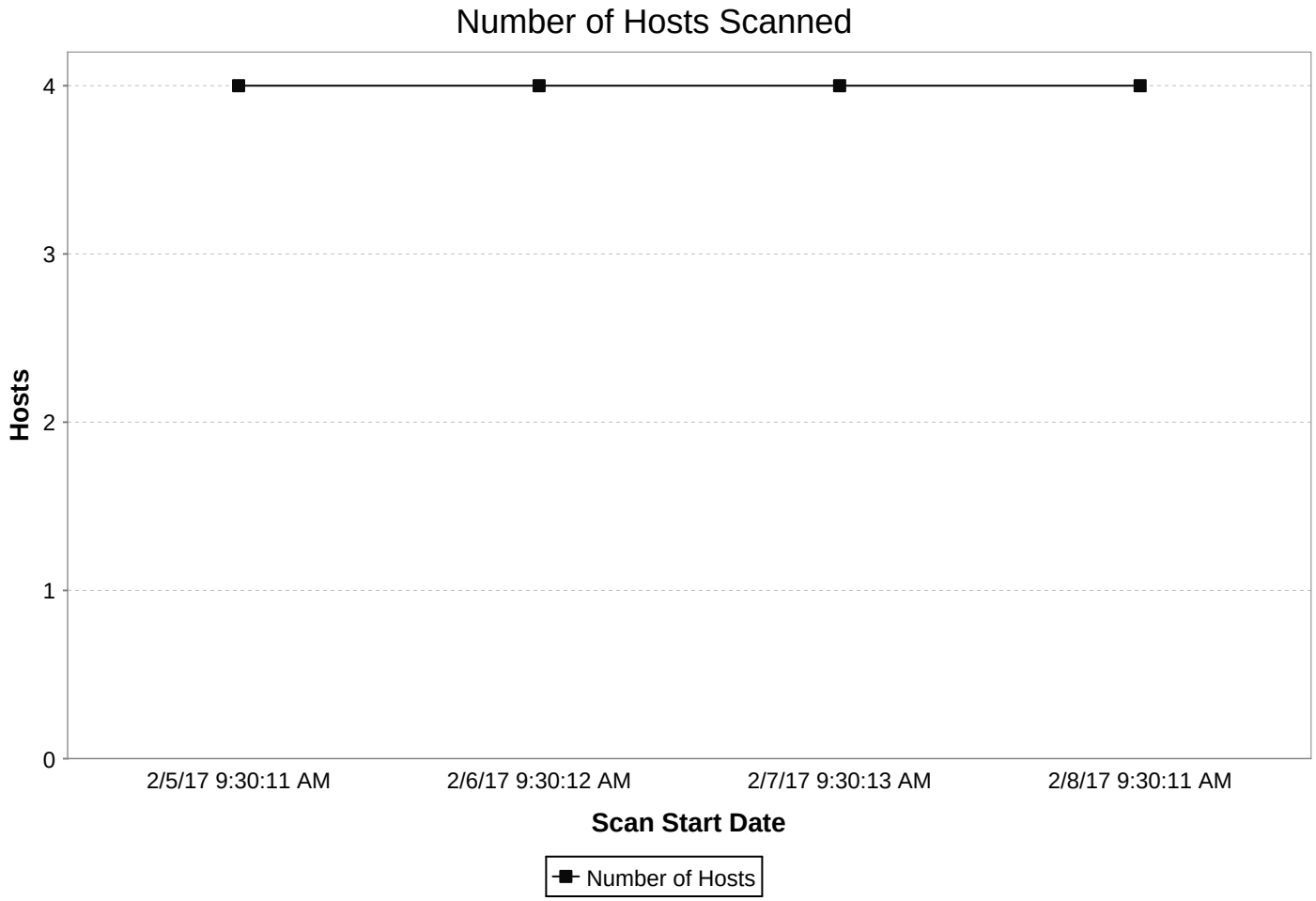
Failed and Error Vulnerabilities by Remediation Status



The chart above shows failed vulnerabilities found for each scan event of the scan named "**feb 2017 daily scan**" broken down by remediation status. Vulnerabilities can be set to one of various remediation statuses (explained below) which represents the status of the work being performed on the latest scan results. As new vulnerabilities are added and as hosts are added to and removed from the network, the amount of vulnerabilities shown will fluctuate. Counts are displayed in the table below.

Unresolved vulnerabilities need attention. **Resolved** vulnerabilities have been addressed and, if successfully remediated, will "pass" when found in future scans. **False Positive** vulnerabilities have been evaluated and are deemed to not be a risk. **Acceptable** vulnerabilities have been evaluated and do not require attention at this time. **Assigned** vulnerabilities need to be addressed by the assigned user but remediation has not yet begun. Vulnerabilities **Under Review** are in the process of being remediated by the assigned user.

	Acceptable	Assigned	False Positive	Resolved	Under Review	Unresolved
2/5/17 9:30:11 AM	**475**	**0**	**452**	**0**	**0**	**20**
2/6/17 9:30:12 AM	**475**	**0**	**452**	**0**	**0**	**508**
2/7/17 9:30:13 AM	**475**	**0**	**452**	**0**	**0**	**508**
2/8/17 9:30:11 AM	**475**	**0**	**452**	**0**	**0**	**639**



The graph above shows the number of devices that have been scanned over time for the scan named "**feb 2017 daily scan**". Counts are displayed in the table below.

	Total
2/5/17 9:30:11 AM	**4**
2/6/17 9:30:12 AM	**4**
2/7/17 9:30:13 AM	**4**
2/8/17 9:30:11 AM	**4**