

Documenting Vulnerability Exceptions

The following procedure should be used to document false positives and mitigation steps within NeXpose.

1. Login to the VMS scanner
2. Scroll to the *Ticket Listing* section of the home page, or select the *Tickets* tab on the Home screen.
3. Under the *Ticket Name* column, look for any newly created tickets prefaced with FP, CC, AU, AR or Other. Select the ticket by clicking on the hyperlinked ticket name.

| Opened | Ticket Name | Device | Status | Priority |
|-----------------|------------------------------------------------------------|--------------------------------|----------------------------|----------|
| Thu Feb 5 2009 | Test Ticket | 130.86.250.16 | Closed - will not be fixed | ☹☹☹ |
| Thu Feb 5 2009 | DNS remediation | 130.86.82.200 | Closed - will not be fixed | ☹☹☹ |
| Tue Feb 17 2009 | HTTP Issues with uprtDwb1 (130.86.243.176) | 130.86.243.176 | Assigned ticket | ☹☹☹ |
| Tue Feb 17 2009 | Secure Services on uprtDwb1 | 130.86.243.176 | Added comment | ☹☹☹ |

4. In the *Ticket Configuration* window select 'Vulnerabilities.

5. Open the device by selecting it's IP address or system name.
6. Under the Vulnerability Listing section, click on the exclude icon in the 'Exclude' column.

Documenting Vulnerability Exceptions

| Vulnerability | Severity | Instances | Exclude |
|------------------------------------------------------------|----------|-----------|---------|
| Obsolete ISC BIND installation | Critical | 1 | |
| Insufficient DNS Source Port Randomization | Severe | 1 | |

Open a ticket

7. In the dialog box that opens
 - a. Select Scope: 'All instances on this device'
 - b. Reason:
 - i. **False Positive** – The vulnerability is being misreported and can be proven using repeatable, documented steps for verification. An example of this would be if a vulnerability is being reported for a service that is not running on the system.
 - ii. **Compensating Control** – The vulnerability is limited in scope by a secondary control. An example of this would be an application vulnerability whose access is limited to a single system with a host based firewall.
 - iii. **Acceptable Use** – The vulnerability being reported falls within the acceptable use policy or best practices of the university.
 - iv. **Acceptable Risk** – The vulnerability cannot be remediated or mitigated and the risk has been explained and accepted by the system owner. Accepted risks must be documented by the system owner.
 - v. **Other** – Must be thoroughly documented in the 'Additional Comments' box.
 - c. **Additional Comments**
 - i. All information supporting the selection of the *Reason* field. This may include system commands run for verification, or change control numbers and/or support tickets.

Documenting Vulnerability Exceptions

Vulnerability Exception

An exception will be created for this vulnerability as follows:

| | |
|---------------------|--------------------------------------------------------------------|
| Vulnerability | Obsolete ISC BIND installation |
| Device | 100.100.102.200 |
| Scope | All instances on this device |
| Reason | False Positive |
| Additional Comments | Compensating Control Acceptable Use Acceptable Risk Other |

Ok Cancel