

Soma Vulnerability Report

```
SELECT hosts.ip_addr, hosts.vlan, hosts.os_hostname, hosts.dns_hostname, os_versions.version_name, vulnerabilities.descr, vuln_id, host_vulnerabilities.discovered_time, host_vulnerabilities.corrected_time, host_vulnerabilities.last_checked_time FROM hosts, os_versions, vulnerabilities WHERE dns_hostname ILIKE ? AND hosts.osver = os_versions.versionid AND host_vulnerabilities.host = hosts.hostname AND host_vulnerabilities.vuln = vulnerabilities.vulnid ORDER BY ip_addr ASC
```

of Records = 13

IP	VLAN	NetBIOS	DNS	OS	Vuln Descr
140.107.74.123	74		VISHNU.FHCRC.ORG	Linux 2.6.X	The remote IPSEC server seems to have a problem negotiating bogus IKE requests. An attacker may use this flaw to disable your VPN remotely Solution: Contact your vendor for a patch Reference : See RFC 2409
140.107.74.123	74		VISHNU.FHCRC.ORG	Linux 2.6.X	It was possible to make the remote web server crash by sending it an invalid HTTP request (GET A) An attacker may use this flaw to prevent this host from fulfilling its role Solution : contact your vendor for a patch
140.107.74.123	74		VISHNU.FHCRC.ORG	Linux 2.6.X	It was possible to freeze or crash Windows or the web server by reading a thousand of times a MS/DOS device through Tomcat servlet engine, using a file name like /examples/servlet/AUX A cracker may use this flaw to make your system crash continuously, preventing you from working properly. Solution : upgrade your Apache Tomcat web server to version 4.1.10.
					It was possible to make the remote host crash by issuing this FTP command : CEL aaaa(...)aaaa This problem is