InfraTrust report: network appliances exposed through PHP2Shell flaws



A report from InfraTrust says attackers are actively exploiting flaws in critical network infrastructure. PHP flaws called PHP2Shell put the web management interfaces of firewalls, VPNs and similar appliances at risk.

- InfraTrust reports active exploitation of vulnerabilities in critical network infrastructure.
- The PHP flaws are referred to as PHP2Shell.
- Affected categories include firewalls, VPNs and application delivery controllers.
- The exposure centres on the web management interfaces of these appliances.
- The source excerpt gives no vendor, CVE or patch details.

What was reported

A report from InfraTrust, covered by BleepingComputer, warns that attackers are actively exploiting vulnerabilities in critical network infrastructure. It highlights a set of PHP flaws known as **PHP2Shell**, which put the web management interfaces of network appliances at risk.

The appliance types named include firewalls, VPNs and application delivery controllers, along with other similar devices. These sit at the network edge and often hold privileged access, so weaknesses in their management layer deserve attention.

What we do not know yet

The available excerpt does not name affected vendors or products, CVE identifiers, severity scores or fixes. Institutions should therefore avoid assumptions about whether a particular device is affected and should check with their suppliers directly.

Practical reading for Saudi institutions

The common thread is exposure of management interfaces. Reducing who can reach them, and confirming the state of each appliance, is a sensible response while fuller details emerge. Teams should also review the original report once the complete text is available.

What to do now

1. Inventory firewalls, VPNs and application delivery controllers, and note which expose a web management interface.
2. Restrict management interfaces to dedicated internal networks or administrative hosts, not the internet.
3. Ask appliance vendors whether their products are affected by PHP2Shell and apply any fixes they release.
4. Review appliance and management logs for unexpected access or configuration changes.
5. Record the issue in the vulnerability and third-party risk registers under your NCA ECC and SAMA CSF processes.