All iDirect Posted Common Vulnerabilities and Exposures (CVE)

CVE ID CVE-2015-0235

1. CVE name: Ghost
2. Affected products and versions: All
3. Fixed products and versions: Velocity 1.1, Pulse 1.1, iDX 3.3.1.0 and later, iDX 2.3.2.0[1] iDX 3.1.1.10 and later

4. Vulnerable installation conditions (e.g., default installation, installation with specific configuration settings, etc.): All installations not patched.

5. Non-vulnerable installation conditions or "workarounds" (e.g., choices of configuration, operating-system platform, etc. that would make exploitation impossible): None

6. Vendor-specific vulnerability identifiers (e.g., any bug number, tracking number, or bulletin number that was previously used in communication with multiple customers about the security issue): CVE-2015-0235, RHSA-2015:0090, RHSA-2015:0092

7. Vulnerability Description and Impact: GHOST is a 'buffer overflow' bug affecting the gethostbyname() and gethostbyname2() function calls in the glibc library. This vulnerability allows a remote attacker that is able to make an application call to either of these functions to execute arbitrary code with the permissions of the user running the application. The gethostbyname() function calls are used for DNS resolving, which is a very common event. To exploit this vulnerability, an attacker must trigger a buffer overflow by supplying an invalid hostname argument to an application that performs a DNS resolution.
8. CVE identifier: CVE-2015-0235
9. Risk/Severity Rating: Critical
10. Vulnerability discoverer: Industry
11. Vulnerability discoverer's web page (if applicable):Industry
12. Disclosure date:
13. Type of disclosure (e.g., coordinated with discoverer or other third party, discovered in the wild through an incident or malware analysis, discovered by vendor QA process, etc.):

[1] The patch required is expected to be released into 2.3.2.0 when development starts.