IC-IRC

Intelligence Community Incident Response Center

(U) IC-IRC Situational Awareness Report

(U//FOUO) Situational Awareness reports contain information on a variety of issues such as general information reports, quarterly/semi-annual/annual summaries, isolated communications outages, other information of value to the IC.

(U) Multiple Vulnerabilities in ArcSight Components Could Cause Remote Disclosure of Information

Date: 18 February 2013
TRACKING NUMBER: ICIRC-SA-023-2013

(U) SUMMARY

(U) Multiple vulnerabilities in ArcSight Connector Appliance and ArcSight Logger could be exploited to allow disclosure of information, command injection and cross-site scripting (XSS). Attackers can modify specific files that are imported by ArcSight to include JavaScript code that will be executed with privileges and permissions associated with the Administrative Console. HP has released patches for these vulnerabilities.

(U) DETAILS

(U) Vulnerable versions of the HP ArcSight software are:

- ArcSight Connector Appliances version 6.3 and earlier
- ArcSight Logger version 5.2 and earlier

(U) In August 2012, it was announced that HP's ArcSight Connector Appliance and Logger contain a file import facility which is vulnerable to cross-site scripting (XSS). When importing a host data file by clicking System Admin Tab > Network > Hosts > Import from Local File, the data is not sanitized before being imported to the ArcSight Connector or Logger Appliances. If an attacker has write access to the host data file that will be imported, that individual can add JavaScript code to the file and it will be run with the permissions and privileges of the administrative web GUI when the file is imported. A remote attacker could trick or entice a user into importing a malicious host file that would give the attacker access to sensitive information and enable him to steal user cookers or escalate privileges.

(U) In February 2013, two recent additional unspecified vulnerabilities were discovered in the vulnerable versions of HP ArcSight software listed above. This additional vulnerability allows remote authenticated users to execute arbitrary code via unknown vectors. At this time, no additional information is available for this vulnerability.

(U) The National Vulnerability Database (NVD) has created the following CVEs in relation to these vulnerabilities: CVE-2012-2960, CVE-2012-3286, CVE-2012-5198, and CVE-2012-5199.

(U) MITIGATION

(U) HP has released software updates to mitigate these vulnerabilities. HP ArcSight Connector Appliance v6.4 and HP ArcSight Logger v5.3 are available by contacting HP to receive information and links for downloading patches.

(U) The IC-IRC recommends that all elements that are using the affected versions of the ArcSight software should install the patches as soon as possible to prevent exploit and compromise of those systems.

(U) To exploit these vulnerabilities, attackers must either deliver a malicious host file to or modify an existing file on a vulnerable system. By ensuring that only authorized personnel are able to access or modify host data files and ensuring that host data files from trusted sources are used, the changes of exploitation are reduces.

(U) SOURCES

"HPSBMU02836 SSRT101056 Rev. 1 – HP ArcSight Connector Appliance and ArcSight Logger, Remote Disclosure of Information, Command Injection, Cross-Site Scripting (XSS)." HP Support Center, Hewlett Packard, 14 Feb. 201. Web. 18 Feb. 2013. http://h20565.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?docid=emr_na-c03606700.

HP ArcSight Logger and Connector Appliances Cross-Site Scripting Vulnerability. Rep. no. 960468. N.p.: n.p., n.d. Vulnerability Notes Database. Web. 18 Feb. 2013. <http://www.kb.cert.org/vuls/id/960468>.

National Vulnerability Database (NVD) National Vulnerability Database (CVE-2012-2960). Rep. no. CVE-2012-2960. N.p., 8 Aug. 2012. Web. 18 Feb. 2013. <http://web.nvd.nist.gov/view/vuln/detail?vulnid+CVE-2012-2960>.

National Vulnerability Database (NVD) National Vulnerability Database (CVE-2012-3286). Rep. no. CVE-2012-3286. N.p., 16 Feb. 2013. Web. 18 Feb. 2013. <http://web.nvd.nist.gov/view/vuln/detail?vulnid+CVE-2012-3286>.

National Vulnerability Database (NVD) National Vulnerability Database (CVE-2012-5198). Rep. no. CVE-2012-5198. N.p., 16 Feb. 2013. Web. 18 Feb. 2013. <http://web.nvd.nist.gov/view/vuln/detail?vulnid+CVE-2012-5198>.

National Vulnerability Database (NVD) National Vulnerability Database (CVE-2012-5199). Rep. no. CVE-2012-5199. N.p., 16 Feb. 2013. Web. 18 Feb. 2013. <http://web.nvd.nist.gov/view/vuln/detail?vulnid+CVE-2012-5199>.

(U) FEEDBACK INSTRUCTIONS

(U) None at this time.

(U) IC-IRC CONTACT INFORMATION

(U//FOUO) **Intelligence Community Incident Response Center (IC-IRC)**
Secure: 984-6371 ♦ Comm: 202-231-8900 ♦
STE: 202-231-8900 ♦ DRSN: 228-7424

(U//FOUO) **IC-IRC Vulnerability Management Program**
Secure 919-3909 ♦ Comm 703-735-5952
ICIRC@dodiis.ic.gov
http://intelshare.intelink.ic.gov/sites/icirc/default.aspx