IOActive Security Advisory

Title	DASDEC Vulnerabilities
Severity	Critical
Discovered by	Mike Davis

Affected Products

DASDEC-I and DASDEC-II from Digital Alert Systems (DAS); other DAS Linux-based platforms may also be affected.

History:

The United States Emergency Alert System (EAS) in 1997 replaced the older and better known Emergency Broadcast System (EBS) used to deliver local or national emergency information. The EAS is designed to "enable the President of the United States to speak to the United States within 10 minutes" after a disaster occurs. In the past these alerts were passed from station to station using the Associated Press (AP) or United Press International (UPI) "wire services", which connected to television and radio stations around the U.S. Whenever the station received an authenticated Emergency Action Notification (EAN), the station would disrupt its current broadcast to deliver the message to the public.

DASDEC is one of a small number of application servers that now fill the role of delivering emergency messages to television and radio stations. DASDEC encoder/decoders receive and authenticate EAS messages delivered over National Oceanic and Atmospheric Administration (NOAA) radio or relayed by a Common Alerting Protocol (CAP) messaging peer. After a station authenticates an EAS message, the DASDEC server interrupts the regular broadcast and relays the message onto the broadcast preceded and followed by alert tones that include some information about the event.

Impact

An attacker who gains control of one or more DASDEC systems can disrupt these stations' ability to transmit and could disseminate false emergency information over a large geographic area. In addition, depending on the configuration of this and other devices, these messages could be forwarded to and mirrored by other DASDEC systems.

Technical Details

The root privileged SSH key for the DASDEC-I and DASDEC-II appliances (and potentially other Linux-based hardware provided by DAS) is distributed as part of the DASDEC firmware. This key would allow an attacker to log in as *Root* over the Internet to a DASDEC device, and then manipulate any system function.

This SSH key is publicly available and cannot be easily removed except by a root privileged user on the server, which is not provided by the DASDEC interface.

```
426167d35dd2ac15145c667c66e1cde7aa2b6c78  authorized_keys2.dasdec

ff687ddcf05ce4357e62ed9676be20d33e6b2a4a  id_dsa.dasdec

426167d35dd2ac15145c667c66e1cde7aa2b6c78  id_dsa.pub.dasdec
```

Additionally, all logged information on a DASDEC server can be accessed by an unauthenticated user. Log access also allows an attacker to browse key directories, providing him with a wealth of information about the server, its administrators, its peering arrangement—and basic login/logout information.

```
e.g.

http://<DASDECADDRESS>/dasdec/op_logs/

http://<DASDECADDRESS>/dasdec/weblogs/

http://<DASDECADDRESS>/dasdec/forwarded_events/

http://<DASDECADDRESS>/dasdec/cap_recv_events/
```

Solution

These findings are not a comprehensive list of the security issues IOActive identified with the DASDEC appliances. The issues described above indicate to IOActive that DAS needs to re-evaluate their firmware and push updates to all appliances to resolve these issues.

Without access to vulnerable devices, patches, etc. it is difficult to provide recommendations on how to properly protect. Please liaise with the vulnerable vendor for guidance.

References

http://www.kb.cert.org/vuls/id/662676