ESA-20180417-04
SmartServer and i.LON 600 Plaintext Passwords

Overview

The SmartServer and i.LON 600 products store passwords in plaintext format. To restrict access to the password file, Echelon recommends that integrators always change the username and password on initial installation, and also recommends that all SmartServers be installed behind a firewall or on a VLAN to minimize exposure to attackers.

Affected Products

All SmartServer 2, SmartServer 1, i.LON 100, and i.LON 600 products.

Vulnerability Overview

The SmartServer and i.LON 600 products are shipped with a default username and password of **ilon** / **ilon**. If the default username or password is not changed when the SmartServer or i.LON 600 is installed in a system, an attacker can use the default username and password to gain access to the SmartServer or i.LON 600 file system via FTP and can replace the SmartServer or i.LON 600 firmware binaries and modules with malicious versions to execute arbitrary code.. In addition, by default the SmartServer **WebParams.dat** file does not restrict access to the SOAP API. For the SmartServer, an attacker can use the SOAP API to retrieve the passwords from the **WebParams.dat** file. Using these usernames and passwords, an attacker can access the SmartServer web user interface and can replace the SmartServer firmware binaries and modules with malicious versions to execute arbitrary code.

Risk Evaluation

The risk is high with the default settings, but can be mitigated by changing the username and password during the initial installation, restricting access to the SOAP API, and locating the SmartServer or i.LON 600 behind a firewall or on a VLAN as described in the next section.

Mitigation

During initial installation, change the username and password. To mitigate the impact of compromised usernames and passwords, assign a unique username and password for every SmartServer and i.LON 600 for sites with multiple SmartServers and i.LON 600s. For the SmartServer and i.LON 100 products, the procedure is described in Appendix C, *Securing the SmartServer*, of the *SmartServer User's Guide*. For the i.LON 600 products, the procedure is described in Appendix E, *i.LON 600 Web Server Parameters Application*, of the *i.LON 600 User's Guide*.

To restrict access to the SOAP API, add an "**/WSDL/*:all:everywhere**" entry under Realms in **WebParams.dat** as described in Appendix C, *Securing the SmartServer*, of the *SmartServer User's Guide*.

With this entry, the Realms entry will look as follows:

```
(Realms)
/user/Echelon/*:all:everywhere
/WSDL/*:all:everywhere
```

To minimize exposure to attackers, install the SmartServer or i.LON 600 and any servers using the SmartServer or i.LON 600 behind a firewall or on a VLAN without other devices. The VLAN approach limits the threat vector from other internal devices and users that are not part of the same system with the SmartServer or i.LON 600 and associated servers. When using a firewall, to minimize threat exposure do not configure the firewall to do any port forwarding to the SmartServer or i.LON 600.

Acknowledgement

Echelon thanks Daniel Crowley and IBM's X-Force Red team for reporting the vulnerabilities.

History

V1.0 (2018-04-17): Initial publication

PGP Signature

To send an encrypted communication to Echelon concerning any security vulnerability questions, reports, or issues, use the following PGP key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFrCu+QBCADim1Dv1Xj+wYUMpniZM0J5Cv9VtBK95NrW3U956p6s6w/WAbBj
c52p4+qF01dmXMg6x14a8lMUDzJxfzW/at6U8HcZp+Kd8TBgmU9xLpZFcb3ey41z
KbcC39c3shL9JnERci5ObB8BHsbNAswhNn7wbpMkgLfLJItxyAYlNK7T9mepO3Rp
WnecyaKT21UWTE2vo1TEB1Jx6P5luCkIHeVVrZZlQmLHY4B6dU1VN4g9ngut/LNx
Rfnu9nfkwAV5sIjW6zmmB6jRSgu+vV2s6rVoyc3ATxViAQDAMMOkSlOdU7gYSOSL
uXyR1bVgOTFhhPVQO+no55z/h/SfDupXqee1ABEBAAG0CFJpY2ggS2V5iQFOBBMB
CAA4FiEEFTDZ9piFJnflLx2IFAu2dl7bl7UFAlrCu+QCGwMFCwkIBwIGFQoJCAsC
BBYCAwECHgECF4AACgkQFAu2dl7bl7VeUAf+Ik9Cqx4Xhyg0P/0MFuvWd9ywqQgk
B3zls+lyBwuwRQnUoWRfWGB/JWK4Ocfe7AjDzAbHcScMuCZniY/Bq1QpuguyeD9K
/d3YM17wkW2pwHkk1xd7yHIkl0g87Uedt4133YOBLU/eUeAVTFQ0QLaFLzbXICO7
h7S3vXsXTao5V2GPeY4AM1i/h3tMUeOXT0ASWCL9S7AQavKnGr8HJX1e+ikj8rVX
icRBA0xcg17aSqRUdyCFJi5W0AaKXDVJSWRz6hszF799PqS/syLqYxYSU+t1uHVd
7Qnq3gPnA+qUZuTzUTqZzMDccxW/MAeazjHik0XK4Nb7BGM8wBkhO8ZT4LkBDQRa
wrvkAQgAsvyLqmDZ+1jwslTUAWLS3sJQxAjtRywgSMxiUJgGDhGYvmOqagGrVmnD
LDS8WnplKtgPpgwKtUY1nIQeYwQ0wrFvkwVX7iokYKWrgBTaiJLVk3SqvGqhb4Nb
8wDLpj6TjOT2B/KqNaT8NS9WVj4VCjOm6eR2R+gM2njVDu3Gl1uLDwQm3VHbJUJG
JTybM0sSUtf/ZOefZkAE0tiCbgMaI7J1slCat9twU+yABLwmcFy/Fk5A+krHSLM2
k5YstWj9CBzTc+LgndTHJNK0fZk0plVG1Jar9+1TArbPEY7e6qlNlaT7BbL9/Dmd
XDyjvx9bP1Xmgk3hZBfzQmr7DvOGGQARAQABiQE2BBgBCAAgFiEEFTDZ9piFJnfl
Lx2IFAu2dl7bl7UFAlrCu+QCGwwACgkQFAu2dl7bl7WORAf/eFQ4TiW0KhxizvFk
Exmkdq3wYU7ymbX5KfCy+jhkhaF8UiR6We2jJ8Ko5ndR7zCy99H8IqSMNQTqCV27
AI/3iRTKXESqzoQdtjCoihtY/ZlqYUVaY2wsaj0mHzzARPXc4EXHxqhyBoqON7uf
U8b0Nxwk6646BpPwl1LqWSNScV2t0yXiJp62YzaGZZ1DN5rXWQL5yUI3O4fOWrfz
OkjbF4miRlXhmrm7dhs9mK9ctNZFYMQoqgacRj7/ASyjcYoSL1M2GXXXqE7IJyiB
C2oIzDaIPgJdurOKrEnWelCj7qIJq4gAfp+WIIFjdCgqgxPGL6O1GTygWetFEETK
UzV1yg==
=mgme
-----END PGP PUBLIC KEY BLOCK-----
```