ESA-20180417-05
SmartServer and i.LON 600 Unencrypted Communications

Overview

Multiple services on the SmartServer and i.LON 600 do not use encryption to protect communications. Both devices allow unencrypted Web connections by default, and both devices can receive configuration and firmware updates by unsecure FTP. Echelon recommends disabling all unsecure services 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 default services that allow unencrypted Web communications by default. An attacker can use unsecure FTP to transfer files to the SmartServer or i.LON 600 to 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 disabling all unrestricted services.

Mitigation

To disable unencrypted services and secure encrypted services for the SmartServer or i.LON 100, follow these steps:

1. Open the **Setup – Security** configuration page as described in the *Configuring Security Properties* section of Chapter 3, *Configuring and Managing the SmartServer*, of the *SmartServer User's Guide*. Clear all checkboxes except the **Enable SSL Web Server**, **Enable Downlink RNI Connections**, and **Enable LonScanner Connections** checkboxes.
2. Create a self-signed TLS certificate or obtain a direct-signed TLS certificate and install it on your SmartServer as described in Using HTTPS/SSL in Chapter 3, *Configuring and Managing the SmartServer*, of the *SmartServer User's Guide*.
3. For the RNI interfaces, set up an MD5 key or secret phrase as described under *Authentication* in *Configuring the SmartServer as a Remote Network Interface* in Chapter 3, *Configuring and Managing the SmartServer*, of the *SmartServer User's Guide*.

To disable unencrypted services and secure encrypted services for the i.LON 600, follow these steps:

1. Open the **Setup – Security** configuration page as described in the *Setting the i.LON 600 Security* section of Chapter 4, *Configuring the i.LON 600 TCP/IP Settings*, of the *i.LON 600 User's Guide*. Clear all checkboxes.

2. For the RNI interfaces, set up an MD5 key as described under *MD5 Authentication* in *Setting the i.LON 600 Security* section of Chapter 4, *Configuring the i.LON 600 TCP/IP Settings*, of the *i.LON 600 User's Guide*.

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
Rfnu9nfkwAV5sljW6zmmB6jRSgu+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-----